HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.
Franz Schwanninger

Analyse der Gesprächsqualität von VoIP in Unternehmensnetzwerken

Mittweida, 2011

Fakultät Elektro- und Informationstechnik

DIPLOMARBEIT

Analyse der Gesprächsqualität von VoIP in Unternehmensnetzwerken

Autor:
Ing. Franz Schwanninger

Studiengang:
Informationstechnik

Seminargruppe:
KI09wIA

Erstprüfer:
Prof. Dr.-Ing. habil. Lutz Winkler

Zweitprüfer:
M.Sc Rico Thomanek

Einreichung:
Mittweida, 28.07.2011

Verteidigung/Bewertung:
Mittweida, 2011

Bibliografische Angaben:

Schwanninger, Franz:
Analyse der Gesprächsqualität von VoIP in Unternehmensnetzwerken – 2011.
Mittweida, Hochschule Mittweida (FH), University of Applied Sciences,
Fakultät Elektro- und Informationstechnik, 68 Seiten, 25 Abbildungen, 8
Tabellen, 2 Anlagen mit Bildern, Diplomarbeit, 2011

Referat:

Mit der zunehmenden Verwendung des Internet Protokolls (IP) für verschiedenste Dienste der Nachrichtenübertragung gewann in den letzten Jahren die Übertragung von Sprache über IP (Voice over IP – VoIP) an Wichtigkeit.
Die vorliegende Diplomarbeit befasst sich hauptsächlich mit den Qualitätsansprüchen an eine professionelle Verwendung in einem Unternehmen. Dabei werden wesentliche Kennwerte der Gesprächsqualität erläutert und deren Aussagekraft bei VoIP abgewogen.
Für ein typisches Einsatzszenario wird die Möglichkeit einer laufenden Qualitätsüberwachung mittels einer quelloffenen und serverbasierenden Lösung behandelt.

Abstract:

With the rising usage of the Internet Protocol (IP) for different services of telecommunications the transmission of Voice over IP (VoIP) has become more and more important within the last years.
This thesis' objectives are the quality demands at a professional environment in a company. Thus, significant values which allow statements about voice quality are explained and their meaningfulness at VoIP are weighted up against each other.
For a typical scenario the possibility of constantly running quality-monitoring with an open-source and server-based solution will be explained.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSD	Berkley Software Distribution
CDR	Call Detail Record
CELP	Code-Excited Linear Prediction
GCC	Gnu Compiler Collection
GSM	Global System for Mobile Communication
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
LAN	Local Area Network
MOS	Mean Opinion Score
PBX	Private Branch Exchange
PCM	Puls-Code Modulation
PHP	Hypertext Preprocessor
PLC	Packet Loss Concealment
QoS	Quality of Service
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
RTT	Round Trip Time
SIP	Session Initiation Protocol
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TK	Telekommunikation
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
VAD	Voice Activity Detection
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

0 Einleitung

Die vorliegende Diplomarbeit wurde auf Basis eines Themas aus dem Umfeld meiner beruflichen Tätigkeit bei der Firma Datentechnik GmbH in Innsbruck im Zeitraum von Feber 2011 bis Juli 2011 angefertigt.

Ich möchte mich bei allen bedanken, die mein Studium möglich gemacht und bei der Entstehung der Arbeit mitgewirkt haben, insbesondere meinem Betreuer Prof. Dr.-Ing. habil. Lutz Winkler und meinen beiden Kollegen Martin und Andreas am Firmenstandort in Innsbruck, von denen ich vieles zu diesem Thema lernen konnte. Außerdem möchte ich Christoph aus unserer Firmenzentrale in Wien danken, der mir als betrieblicher Betreuer einige Tipps zum Verfassen meiner Arbeit gab, und meinem Chef Wolfgang, der mir mein Studium durch seine Unterstützung innerhalb der Firma ermöglichte.

0.1 Motivation

Eine der Herausforderungen bei der Verwendung von VoIP in einem professionellen Umfeld ist es, in IP-Umgebungen ein konstant gutes Maß an Gesprächsqualität aufrechtzuerhalten. Die Ursachen für Probleme können dabei unterschiedlich sein; so wirken sich zum Beispiel die Verwendung von stark komprimierten Audiocodecs oder vielfältige Probleme mit der Netzwerkverbindung, die technischen oder organisatorischen Ursprungs sein können, negativ auf die Qualität eines Gesprächs aus.

Insbesondere für Techniker oder administratives Personal ist es deshalb wichtig, Möglichkeiten zu haben, um solche Fälle analysieren und dementsprechend reagieren zu können. Es ist zunächst von Interesse, ein bestehendes oder bereits in der Vergangenheit aufgetretenes Problem bei einer Gesprächsverbindung nachvollziehen zu können. Weiters soll auf derartige Probleme aufgrund vorliegender Informationen reagiert werden können, um die Ursache zu finden und zu beseitigen.

Spezielle Werkzeuge zur Analyse und Problembehebung sind nützlich, weil herkömmliche Netzwerkverwaltungslösungen üblicherweise nicht alle Aspekte von Sprachübertragung abdecken können, und da schlechte Gesprächsqualität bei VoIP nicht immer mit allgemeinen Netzwerkproblemen einhergeht.

0.2 Abgrenzung

Im Rahmen der vorliegenden Arbeit sollen nur die Gesichtspunkte der Sprachübertragung betrachtet werden, die in typischen Unternehmensnetzwerken relevant sind. Ausgegangen wird dabei von einem Netzwerk, das im lokalen Netz (Local Area Network – LAN) aus moderner Infrastruktur, basierend auf Ethernet, basiert. Als Protokoll auf der Netzwerkschicht wird dabei nur IP verwendet.

Als betrachtete Topologien und Testszenarien werden nur ausgewählte Verbindungstypen verwendet, deren Auswahl es zum Ziel hat, ein möglichst breites Spektrum an realen Gegebenheiten wiederzugeben.

Genauso wird mit der dargestellten Auswahl an Sprachcodecs, Protokollen, Telefonanlagen und Endgeräten verfahren. Es wird nicht Anspruch auf eine vollständige Wiedergabe aller existierenden Technologien erhoben; es wird nur eine für die Behandlung der Problemstellung ausgewählte Menge behandelt.

Die dargestellte Lösung mit Nagios und Splunk ist nur eine von vielen Möglichkeiten, diese oder ähnliche Aufgabenstellungen zu lösen. Andere Lösungen können im Rahmen dieser Arbeit nicht behandelt werden.

Außerdem wird in allen Abschnitten nur auf standardbasierende und freie Protokolle eingegangen, wobei speziell in Bezug auf Softwarelösungen der Fokus auf quelloffenen Varianten liegt. Auf die Verwendung proprietärer Lösungen wird, soweit das möglich ist, bewusst verzichtet.

0.3 Kapitelübersicht

Die Grundlagen von VoIP werden in **Kapitel 1** behandelt. Einführend werden die grundlegenden Bedürfnisse der Kunden dargestellt und wie diese mit verschiedenen Herstellern umgesetzt werden können. Nach einer kurzen Beschreibung eines Basisszenarios werden die Möglichkeiten verschiedener Protokolle abgewogen, einige Verfahren der Sprachcodierung sowie Quality of Service erläutert und wichtige Skalen zur Darstellung von Qualität in VoIP behandelt.

Kapitel 2 konzentriert sich auf die Qualitätseinflüsse, die aufgrund der Übertragung mit IP entstehen. Hier wird auf die organisatorischen Probleme eingegangen, auf direkte Einflüsse von Netzen auf den Paketfluss und auf Qualitätsunterschiede bei Endgeräten. In allen Abschnitten des Kapitels werden ausschließlich Kriterien im Zusammenhang mit IP behandelt, auf eine weitere Betrachtung der Analogtechnik wird verzichtet.

In **Kapitel 3** wird eine mögliche Lösung zur Überwachung der Qualitätsansprüche in einem Unternehmen dargestellt. Dabei wird zunächst ein Anwendungsszenario, wie es bei einem Unternehmen mit mehreren Standorten üblich ist, geschildert. Die praktische Umsetzung einer Überwachungslösung unter Verwendung der quelloffenen Lösungen Nagios und Splunk wird genauer beschrieben.

In **Kapitel 4** werden die Ergebnisse und die daraus resultierenden Messwerte sowie entsprechende Darstellungsmöglichkeiten der Lösung erläutert. Weiters werden einige Vorschläge für eine bestmögliche Implementierung aufgezeigt.

Kapitel 5 gibt eine Zusammenfassung und einen Ausblick auf die weitere Entwicklung und Relevanz der Lösung sowie auf die Entwicklung von Qualitätsansprüchen bei VoIP an sich.

Anlagen, Teil 1 zeigt eine Schritt-für-Schritt-Anleitung der Installation von NConf auf einer bestehenden Nagios-Installation, ergänzend zur vorhandenen Onlinedokumentation.

In **Anlagen, Teil 2** sind alle Syslog-Meldungen der behandelten Beispiele für Rufverläufe zu finden.

1 VoIP – Technische Grundlagen

Es gibt viele Faktoren innerhalb eines VoIP-Systems, welche die Gesprächsqualität beeinflussen können. Beispiele hierfür sind vor allem der verwendete Sprachcodec, aber auch die Verfahren zur weiteren Bearbeitung der Sprachdaten können Auswirkungen zeigen. In diesem Abschnitt werden technische Grundlagen, die für die Betrachtung der Gesprächsqualität in einem Unternehmen relevant sind, betrachtet.

1.1 Überblick über Komponenten und Anbieter

In diesem Abschnitt wird eine Übersicht über die Bestandteile eines Systems sowie aktuell verfügbare und verbreitete Lösungsansätze verschiedener Hersteller zur Realisierung von Kundenanforderungen gegeben. Weiters werden allgemeine Möglichkeiten zur Vernetzung der einzelnen Bestandteile dargestellt.

1.1.1 TK-Anlagen

Am Markt befindet sich derzeit eine Vielzahl an Anbietern von TK-Anlagen (Telekommunikation – TK), welche die Grundlage einer Installation bieten. Die Hersteller verfolgen dabei häufig unterschiedliche Lösungsansätze und Herangehensweisen an die Aufgabenstellungen, die VoIP mit sich bringt. Diese lassen sich im Zuge dieser Betrachtung in zwei Hauptgruppen einteilen:

- Hersteller, deren Implementierung vorwiegend auf proprietären Technologien basieren
- Hersteller, die sich bei ihren Implementierungen nach Standards von ITU (International Telecommunication Union) und IETF (Internet Engineering Task Force) richten

Zur ersten Gruppe zählen hauptsächlich große Hersteller wie Cisco Systems, Alcatel, Siemens, Microsoft oder Nortel. Deren Lösungen greifen häufig auf eine lange Tradition an technisch aufwändigen und umfangreichen Implementierungen zurück. Aus diesem Grund sind VoIP-TK-Anlagen in der Vergangenheit oft direkt aus herkömmlichen TK-Anlagen entstanden, wodurch sich auch viele mittlerweile veraltete Aspekte der Analogtelefonie im Zeitalter des Internetprotokolls (IP) lange gehalten haben. Das Ergebnis sind meist optisch ansprechende und erprobte Geräte und Telefonanlagen mit vielen Funktionen, die für den Konsumenten in der Regel aber kostspielig sind. Zu den Kunden oben genannter Unternehmen zählen deshalb häufig größere Unternehmen oder staatliche Einrichtungen.

Im Vordergrund stehen bei den Herstellern Lösungen, die in einem geschlossenen System viele Funktionen bieten können. Die Kompatibilität zu anderen Herstellern ist hier nicht so wichtig. Der Einsatz einer Mischlösung verschiedener Hersteller, insbesondere Telefonanlagen in verschiedenen Lokationen, die miteinander kommunizieren, ist nicht vorgesehen oder gar nicht möglich. Dahinter steht teilweise eine Strategie des Herstellers, der eine gemischte Lösung nicht unterstützt und das mit den Mitteln proprietärer Technik durchsetzt.

Zur zweiten Gruppe zählen sowohl kleinere und weniger etablierte Hersteller wie Innovaphone, Snom, oder Aastra, als auch quelloffene Lösungen wie der populäre Asterisk-Server.

Hersteller dieser Gruppe können oft nicht auf eine langjährige Erfahrung mit Telefonie zurückblicken, was Nachteile, aber auch Vorteile mit sich bringt. Zunächst können diese Hersteller selten auf langjährige Kundenbeziehungen zurückgreifen und sind so bei der Verbreitung der Produkte eher auf Aquisition von Neukunden angewiesen, was sich als schwierig herausstellt. Als Vorteil von „jungen“ und meist kleineren TK-Herstellern ist zu werten, dass die Erfolgsgeschichte von VoIP von Beginn an einen maßgeblichen Einfluss auf die Entwicklung dieser Systeme genommen hat. Deshalb sind die Systeme generell bei ähnlichem Funktionsumfang einfacher und kostengünstiger, weil nur moderne Anforderungen an eine TK-Anlage implementiert wurden, und auf die Realisierung mittlerweile veralteter Funktionen verzichtet wurde.

Aufgrund der strategischen Platzierung dieser Produkte sowie oftmaliger Realisierungen von Teilsystemen ist Kompatibilität zu anderen Herstellern, insbesondere bestehender Installationen von Fremdherstellern, sehr wichtig. Das wird zunächst durch eine einfache Grundsatzentscheidung der Hersteller erreicht: Bei der Entwicklung hält man sich streng an Standards. Nur Funktionen, für die keine ausreichende Spezifikation in einem bestehenden Standard existiert, werden durch eine proprietäre Lösung abgebildet. Das Ergebnis sind Produkte, die einen hohen Grad an Kompatibilität untereinander und zu anderen Lösungen aufweisen und so mit einigem technischen Aufwand auch sehr flexibel und anpassbar sind.

1.1.2 Externe Softwarelösungen

Für Unternehmen sind heute nicht nur grundlegende Funktionen von TK-Systemem wie einfache Rufe wichtig. In den letzten Jahren sind viele zusätzliche Anforderungen an solche Systeme entstanden. Dazu gehören unter anderem Sprachaufzeichnung, Callcenter-Anwendungen, Computer Telephony Integration (CTI), Unified-Messaging-Dienste (UM) sowie die Anbindung externer Überwachungslösungen. In vielen Fällen sind nicht alle Anforderungen durch einen einzigen Hersteller von TK-Anlagen abzubilden, weshalb nicht zugehörige, also externe Softwarelösungen verwendet werden müssen, auch bekannt als „Third-Party-Lösung“. Diese sind für gewöhnlich auf einem herkömmlichen Betriebssystem wie Microsoft Windows oder ausgewählten Linux-Distributionen lauffähig und so in bestehende, gegebenenfalls virtuelle Server-

Infrastrukturen einzubinden. **Abbildung 1-1** zeigt einen Überblick über die wichtigsten Zusatzanforderungen, die auf Servern als externe Softwarelösung realisierbar sind.

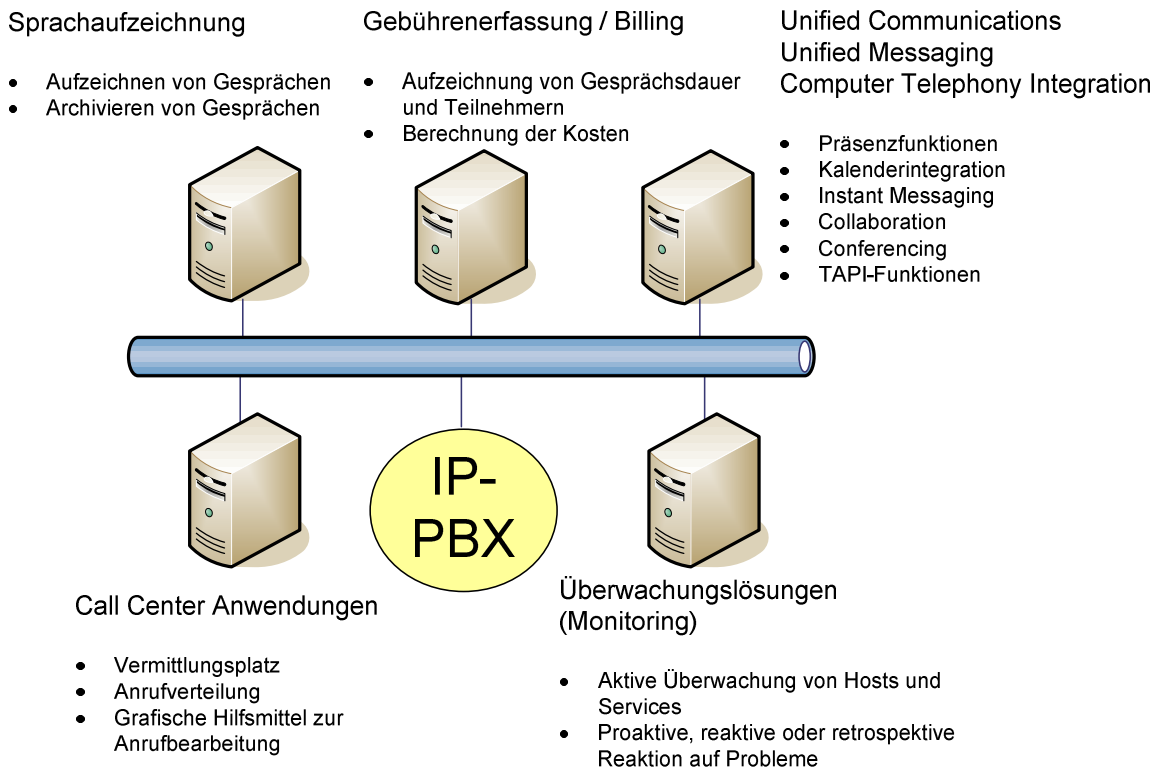


Abbildung 1-1: Externe Softwarelösungen in Unternehmen

Wie im vorigen Abschnitt geschildert, verhalten sich die Schnittstellen zu diesen externen Anwendungen auch unterschiedlich. Bei offenen Systemen ist es mit entsprechendem Aufwand recht einfach, externe Software anzubinden. Bei proprietären Lösungen stellt sich das als problematisch heraus; es kann oft nur die Software desselben Herstellers verwendet werden. Die Implementierung von Standardlösungen ist hier aber, wenn auch seltener, ebenfalls möglich.

1.2 Basisszenario

Ein typisches Einsatzszenario von VoIP besteht zumindest aus einer Telefonanlage, im Folgenden als PBX (Private Branch Exchange) bezeichnet, die mittels geeigneter Funktionen notwendige Dienste erfüllt. Für gewöhnlich ist eine PBX an mindestens einem Punkt mit einem Gateway an das öffentliche Telefonnetz angebunden. Ein optionaler Bestandteil ist die Multipoint Control Unit (**MCU**), die der Verwaltung von Konferenzen mit drei oder mehreren Teilnehmern dient.

→ Die **PBX** stellt lokale Dienste wie Registrierung, Rufaufbau, Rufweiterleitung und Verzeichnisse zur Verfügung. Diese Anforderungen werden bei H.323 mit einem

Gatekeeper realisiert, bei SIP (Session Initiation Protocol) werden Komponenten wie Proxy-, Redirect-, Registrar- oder Locationserver verwendet.

→ Das **Gateway** definiert in diesem Fall einen Übergang von IP zum Transportmedium des öffentlichen Netzes, deshalb stellt es typischerweise Schnittstellen für ISDN (Integrated Services Digital Network) oder analoge Übertragung zur Verfügung.

Entfällt der Einsatz dieser zusätzlichen physikalischen Schnittstellen beispielsweise durch die Verwendung von reiner IP-basierender Telefonie mittels einer Anbindung an einen SIP-Provider, werden die Funktionen des Gateways entsprechend vereinfacht.

Abbildung 1-2 stellt das Basisszenario mit wichtigen Komponenten und Schnittstellen dar.

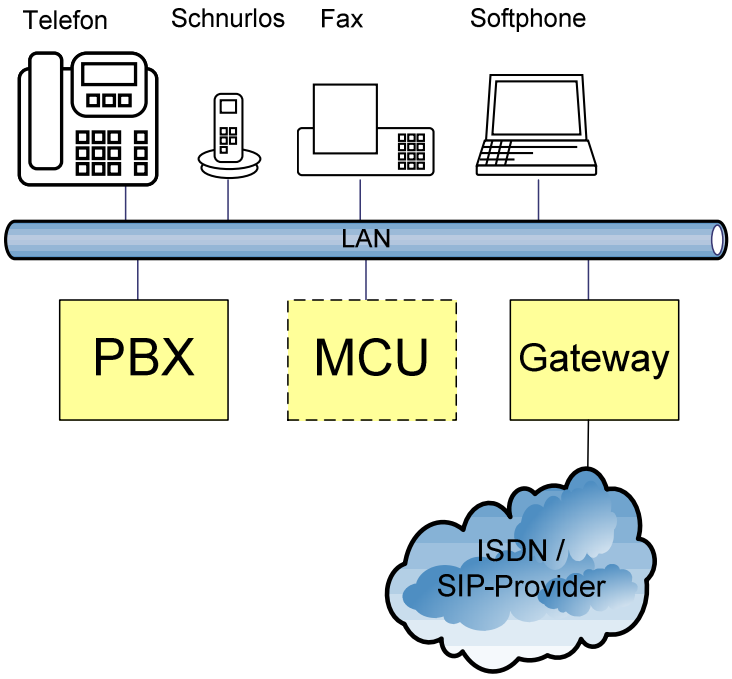


Abbildung 1-2: Basisszenario von VoIP in einem Unternehmen

1.3 Signalisierungsprotokolle

Als Signalisierungsprotokoll gilt eine Zusammenfassung aus Regeln, nach denen Gespräche auf- oder abgebaut werden können. Grundsätzlich sollten die Protokolle darauf ausgelegt sein, diese Basisdienste verlässlich zur Verfügung zu stellen.

Desweiteren werden viele unterschiedliche Zusatzdienste wie Weiterverbinden, Anrufumleitung, Halten oder Anklopfen realisiert.

Auf einen genaueren Vergleich der Zusatzdienste wird hier verzichtet.

1.3.1 VoIP nach H.323

Als Standard der ITU-T ist H.323 ein Rahmenwerk (Framework) aus mehreren weiteren Standards wie H.225.0, H.245, H.450 und H.235. Zusammengefasst stellen H.225.0 und H.245 die notwendigen Mittel zur Signalisierung zur Verfügung. H.450 realisiert ergänzende Dienste (Supplementary Services) und H.235 stellt Mittel zur Authentifizierung und Sicherung zur Verfügung. Die erste Version von H.323 (H.323v1) wurde im Jahr 1996 verabschiedet. Die aktuellste Version ist H.323v7, die 2009 fertig gestellt wurde. /Badach2007/

Die Entwicklung von H.323 ist stark geprägt durch den Einfluss von ISDN: So findet man beispielsweise das ISDN-Protokoll Q.931 im H.323-Protokoll wieder.

Abbildung 1-3 zeigt einen Überblick über die Protokollfamilie und deren Integration in den TCP/IP-Protokollstack. Wie hier ersichtlich ist, wird für die wichtigen Dienste für den Auf- und Abbau des Sprachkanals mit H.245 Control und H.225.0 Call Control, TCP (Transmission Control Protocol) als Transportprotokoll verwendet. Für Dienste, die nicht so empfindlich gegenüber Paketverlust sind, werden verbindungslose UDP-Sitzungen (User Datagram Protocol) verwendet.

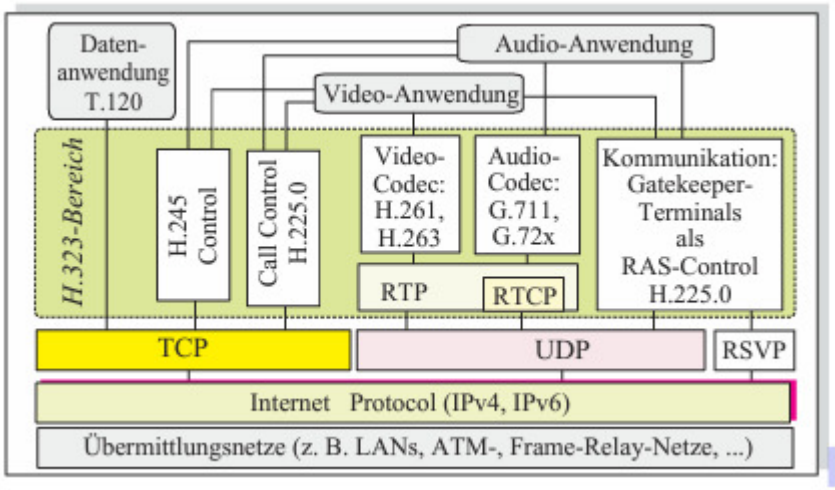


Abbildung 1-3: Protokollfamilie TCP/IP und H.323 -Komponenten. /Badach2007/, S.199

1.3.2 VoIP nach SIP

SIP ist eine Spezifikation der IETF (Internet Engineering Task Force), die sich zwar die Lösung ähnlicher Aufgaben wie H.323 als Ziel setzt, jedoch einen anderen Ansatz verfolgt. Das Konzept von SIP ist sehr einfach und die Nachrichten haben, vom Aufbau her, große Ähnlichkeiten mit HTTP. So kann ein Rufaufbau mit SIP beispielsweise mit dem Aufruf einer Webseite verglichen werden. Wie in **Abbildung 1-4** dargestellt, wird für die Übertragung der Sprachdaten wie bei H.323 als Transportprotokoll UDP verwendet. Für die Signalisierung ist in der Empfehlung der IETF kein Protokoll fest vorgeschrieben. Hier können von Herstellern entweder UDP oder TCP verwendet werden. /Badach2007/, /IETF2011/

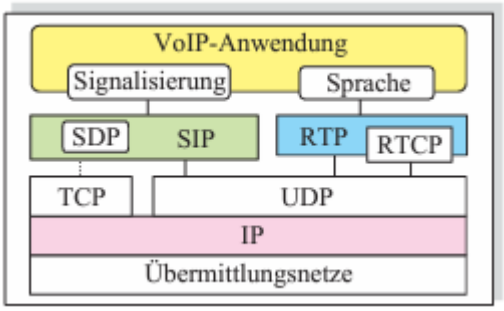


Abbildung 1-4: Protokollfamilie TCP/IP und SIP-Komponenten. /Badach2007/, S.248

Aus der wahlweisen Implementierung von TCP oder UDP ergeben sich zwei verschiedene Ausführungen von SIP, die untereinander nicht kompatibel sind:

- SIP mit UDP (auch: SIP, SIP/UDP)

  Da die meisten Implementierungen von SIP auf UDP als Transportprotokoll zurückgreifen, wird üblicherweise nur die Bezeichnung „SIP“ für die Verwendung von SIP mit UDP verwendet.

- SIP mit TCP (auch: TSIP, SIP/TCP)

  Einige Hersteller implementieren anstelle von UDP das Protokoll TCP, um bei der Signalisierung eine mit H.323 vergleichbare Verlässlichkeit zu erreichen.

1.3.3 Bewertung der Protokolle

Mit allen oben genannten Protokollen können die Grundanforderung an eine VoIP-Installation erfüllt werden.

Im Hinblick auf die Sicherung der Gesprächsqualität ist neben der Erfüllung der notwendigen Signalisierungsfunktionen auch wichtig, ob der Signalisierungsdienst verlässlich erbracht werden kann. Insbesondere stellt es sich hier als problematisch heraus, wenn das Protokoll empfindlich auf Störfälle reagiert, die Paketverlust zur Folge haben.

Die Verwendung von UDP als Transportprotokoll bei SIP führt dazu, dass bei Verlust eines Pakets auf der Übertragungsstrecke weder der Absender noch der Empfänger davon in Kenntnis gesetzt werden. Bei VoIP hat dies zur Folge, dass im Fall von Paketverlust beispielsweise ein Gespräch gar nicht zustande kommt.

Lösungen für dieses Problem können sein, dass

- TCP anstelle von UDP verwendet wird, wie es bei SIP/TCP oder H.323 gelöst wird.

- eine sichernde Funktion, wie sie durch TCP gegeben wird, auch mit dem SIP-Protokoll selbst abgebildet wird. Dies wird beispielsweise durch einen erneuten Versuch des Verbindungsaufbaus nach einem gewissen Zeitablauf erreicht.

Solche Maßnahmen müssen aber von einem Hersteller auf Applikationsebene ergriffen werden, da sie nicht im Standard definiert sind.

→SIP mit UDP ist ohne weitere Maßnahmen zur Transportsicherung anfällig für die Folgen von Paketverlust.

1.4 Quality of Service (QoS) in IP-Netzen

Der typische Ansatz notwendige Bandbreite zu garantieren, um die gewünschte Qualität der Übertragung zu erreichen, wird durch die Umsetzung von QoS-Merkmalen realisiert.

Diesen liegen als Ausführungen von Priorisierung der Sprachdaten gegenüber restlicher Datenübertragung folgende Varianten zugrunde:

- **QoS auf OSI-Layer 2:**

  Diese Variante wird mittels Priorisierung eines Virtuellen LANs (VLANs) nach 802.1p realisiert. Das priorisierte VLAN ist dabei für Sprachdaten reserviert, wobei das Verfahren allerdings nur in LANs angewandt werden kann.

- **QoS auf OSI-Layer 3:**

  Die Integration von QoS-Merkmalen im IP-Header ermöglicht Priorisierung über ein LAN hinweg und kann theoretisch die notwendige Bandbreite zwischen beliebigen Endpunkten im Internet garantieren.

Wenn zur Standortvernetzung ein Internet Service Provider (ISP) benötigt wird, ist es zwischen verschiedenen Standorten eines Unternehmens schwierig, QoS durchgehend zur Verfügung zu stellen. Die Umsetzung von QoS bedarf unter Umständen erheblichem finanziellen Aufwand, weshalb in vielen Fällen, selbst bei professioneller Verwendung in einem Unternehmen, darauf verzichtet wird.

Bei der Standortvernetzung über die Landesgrenzen hinaus ist es unter Umständen durch mangelnde Unterstützung durch den ISP gar nicht möglich.

Als Resultat sind in der Praxis oftmals Netze in Anwendung, die zwar in lokalen Netzen QoS garantieren können, aber die Vernetzung der Standorte untereinander keine Priorisierung erlaubt. Aus diesem Grund sind meist standortübergreifende Gespräche von Qualitätsproblemen betroffen.

1.5 Einführung in Verfahren der Sprachcodierung

Im Folgenden wird eine heute relevante Auswahl an Codecs genauer behandelt und im Hinblick auf deren Sprachqualität und deren bestimmende Faktoren genauer betrachtet. Weiters werden einige Verfahren erwähnt, die in naher Zukunft mehr an Wichtigkeit erlangen werden. Wie in **Abbildung 1-5** dargestellt, funktioniert jedes Verfahren der Sprachcodierung nach dem gezeigten Schema. Die wesentlichen Unterschiede zwischen den Verfahren sind durch verschiedene Realisierungen der Funktionen des dargestellten Blocks „Codierung“ gegeben. Außerdem können Abtaster verschiedener Abtastfrequenzen verwendet werden, wobei hier Werte von 8 KHz (für Narrowband Codecs) oder 16 KHz (für Wideband Codecs) besonders verbreitet sind.

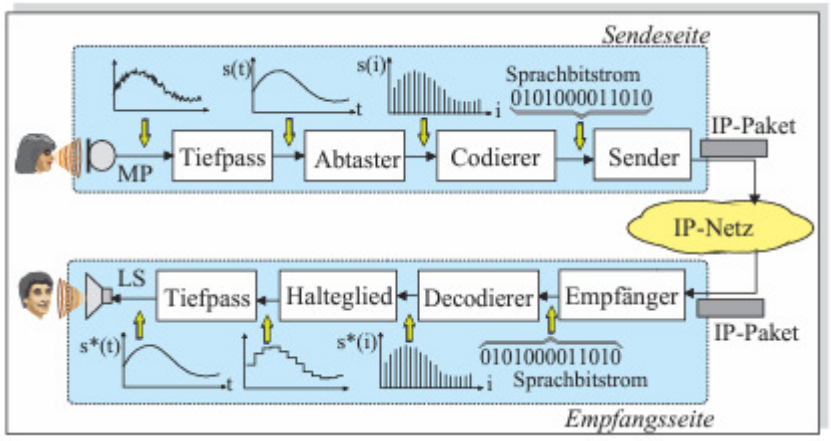


Abbildung 1-5: Grundlegendes Prinzip der Sprachübermittlung über ein IP-Netz /Badach2007/, S.132

1.5.1 Begriffsdefinition

Die im Folgenden öfters verwendete Bezeichnung „Codec“ ist ein Kunstwort aus „Coder“ und „Decoder“ und besagt, dass ein Verfahren somit auf der Sende- und Empfangsseite zum Einsatz kommt. Der Ausdruck „Sprachcodec“ bezeichnet eine Untermenge von Codecs, die für die Übertragung von menschlicher Sprache besonders geeignet ist, aber in der Regel keine hochwertige Übertragung von allgemeinen Audiodaten wie Musik gewährleistet. /Wiki2011/

Weiters sind aus dem englischen Sprachraum die Ausdrücke „Narrow Band Codec“ (Schmalbandcodec) und „Wide Band Codec“ (Breitbandcodec) gebräuchlich. Auf die Eigenschaften der Verfahren wird in den folgenden Abschnitten genauer eingegangen.

1.5.2 Klassifizierung von Sprachcodecs

Allgemein lassen sich Sprachcodierungen aufgrund mehrerer Gesichtspunkte in verschiedene Kategorien einteilen.

1.5.2.1 Unterscheidung zwischen statischen und dynamischen Codecs

- **Sprachcodecs mit fester Codierung und Datenrate**

  Zu diesen gehören hauptsächlich einfachere und gut standardisierte sowie vielfach implementierte Methoden mit fixem Codierungsverfahren bei konstanter Bitrate. Daraus folgt eine leichte Vorhersehbarkeit des Verhaltens. Dazu gehören die Codierungsverfahren der ITU-T, die in **Abschnitt 1.5.3** näher behandelt werden.

- **Sprachcodecs mit dynamisch wechselnder Codierung und Datenrate**

  Zu diesen gehören komplexere Verfahren, die eigentlich mehrere unterschiedliche Codierungsverfahren beinhalten. Automatische Methoden, die Bestandteil der Implementierung sind, können zwischen Verfahren mit hoher oder niedriger Kompressionsrate wechseln. Zu dieser Kategorie gehört der freie Codec Speex, das patentierte Verfahren „Silk“ von Skype Technologies S.A. oder der in Mobilfunknetzen verwendete Adaptive Multirate Codec (AMR).

1.5.2.2 Klassifizierung nach Abtastraten

- **Sprachbandcodecs (Schmalbandcodecs, Narrow Band Codecs)**

  Der klassische Ansatz zur Codierung von menschlicher Sprache sieht einen erfassten Frequenzbereich der Sprache von 300 Hz bis 3400 Hz vor, was nach Berücksichtigung von Shannons Abtasttheorem in einer Abtastrate von 8 KHz resultiert.

- **Breitbandcodecs (Wide Band Codecs)**

  Durch Implementierung moderner Breitbandcodecs wird die Gesprächsqualität mittels der Verwendung höherer Abtastraten erhöht. Typische Werte liegen hierfür zwischen 16 KHz und 48 KHz.

1.5.2.3 Klassifizierung nach Codierungstechnik

- **Abtastwertorientierte Verfahren**

  Einfache Methoden leiten die Ergebnisse der Codierung direkt aus den Abtastwerten ab. Dazu gehören alle Verfahren, die auf Puls-Code-Modulation (PCM) basieren, wie differenzielle oder adaptive/differenzielle PCM (DPCM, ADPCM).

- **Segmentorientierte Verfahren (auch: parametrische Verfahren)**

  Komplexe und aufwändigere Verfahren basieren auf Linear Predictive Coding (LPC), das die Abtastwerte mittels Verfahren der digitalen Signalverarbeitung mit Parametern beschreibt und ersetzt. Zu dieser Kategorie zählen Verfahren wie

Code Excited Linear Prediction (CELP), die höhere Komprimierungsgewinne als abtastwertbasierende Codecs erlauben. Sie benötigen jedoch mehr Rechenleistung, was aber bei heutigen Endgeräten selten ein Problem darstellt.

1.5.3 Sprachcodierung mit standardisierten Verfahren der ITU /Badach2007/

Die ITU-T bietet eine Vielzahl an standardisierten Verfahren zur Sprachcodierung an. Die Bezeichnung gängiger Standards beginnt, wie bei der ITU üblich, mit dem Buchstaben „G“. Nicht jede der Spezifikationen schafft es dabei zu breiter Akzeptanz, viele davon gelten mittlerweile als veraltet oder wurden von Herstellern gar nicht implementiert. Allgemein betrachtet sind die Bezeichnungen G.710 bis G.729 für die Codierung von Sprache und Audio vorgesehen. Zusätze zu den Standards (Annexe) werden durch einen Buchstaben am Ende bezeichnet, wie beispielsweise bei G.729A.

1.5.3.1 Referenzcodec – G.711

Der in diesem Anwendungsgebiet am stärksten etablierte und zugleich einfachste Codec ist G.711 in seinen Varianten G.711 A-Law (auch: G.711a) und G.711 µ-Law (auch: G.711 u-Law oder G.711u), wobei sich G.711 A-Law am europäischen und G.711 µ-Law am amerikanischen und asiatischen Markt durchgesetzt haben. Die Unterschiede zwischen den Varianten sind minimal und die Gesprächsqualität ist bei beiden Verfahren nahezu identisch. Dennoch sind sie untereinander nicht kompatibel.

G.711 ist in den Anfängen von VoIP direkt aus der Codierung von Sprache in ISDN entstanden und ist deshalb bei guten Bedingungen in einem IP-Netz mit der Qualität von ISDN gleichzusetzen. Gleichzeitig ist die Technik, die G.711 zugrunde liegt, der Ausgangspunkt für die Entwicklung einer Vielzahl anderer Codecs. G.711 ist dabei als nichtlineare PCM mit einer Abtastrate von 8 KHz und einer resultierenden Bitrate von 64 Kbit/s ausgeführt.

Somit ist dieser Codec eine gute Wahl für lokale Netze, die über ISDN ans öffentliche Telefonnetz angebunden sind, da bei genug verfügbarer Bandbreite bestmögliche Qualität erreicht wird.

1.5.3.2 Komprimiertes Verfahren – G.729

Eines von vielen Verfahren mit vergleichbar reduzierter Datenrate ist G.729. Dieser Codec ist von hoher Wichtigkeit, weil er als guter Kompromiss zwischen benötigter Bandbreite und erreichter Gesprächsqualität gilt.

Die Implementierung von G.729 ist wesentlich komplexer als jene von G.711, was in erhöhtem Berechnungsaufwand bei der Sprachcodierung resultiert.

Weiters existieren für G.729 einige Zusatzspezifikationen (Annexe), die beispielsweise auf Sprachpausenerkennung genauer eingehen oder einen reduzierten Berechnungsaufwand bei der Sprachcodierung ermöglichen.

Als Grundlage für G.729 gilt das segmentorientierte Verfahren CS-ACELP (Conjugate Structure – Algebraic Code Excited Linear Prediction), welches das Sprachsignal ebenfalls mit einer Abtastrate von 8 KHz berücksichtigt und dabei eine Datenrate von 8 Kbit/s erzeugt.

G.729 ist eine gute Wahl für Netze, in denen die verfügbare Bandbreite limitiert ist, aber trotzdem bestmögliche Qualität erreicht werden soll.

1.5.3.3 Weitere standardisierte Codecs der ITU-T /Wiki2011/, /Sauter2011/

Andere Vertreter der von der ITU-T spezifizierten Codecs sind G.723.1, G.726 und G.728. Jene Verfahren sind in Bezug auf Bandbreitenbedarf und Qualität im Vergleich zu G.711 reduziert, werden in Unternehmensnetzen aber nur teilweise eingesetzt. Der Grund hierfür ist, dass andere Varianten wie G.729 einen besseren Kompromiss zwischen minimalem Bandbreitenbedarf und bestmöglicher Qualität bieten.

Eine Ausnahme ist beispielsweise der Standard G.722, der durch erhöhte Abtastfrequenz die Qualität von G.711 bei gleicher oder niedrigerer Datenrate übertrifft. Die Relevanz von G.722 ist in der Praxis jedoch reduziert, weil G.722 andere Anforderungen an die Analogtechnik in Endgeräten als G.711 hat. Weiters geht der Qualitätsvorteil von G.722 ganz verloren, wenn ein Gespräch über ein öffentliches Netz in G.711-Qualität geführt wird. Aus diesen Gründen werden G.722 und vergleichbare Codecs mit erhöhten Abtastfrequenzen in Unternehmensnetzwerken nur punktuell eingesetzt.

Weiters gibt es eine Vielzahl an Codierungsverfahren, die in mobiler Kommunikation (Global System for Mobile Communication – GSM, Universal Mobile Telecommunication System – UMTS) angewandt werden. Jene sind für die Anwendung in Unternehmensnetzen jedoch nicht relevant.

1.5.4 Alternativen zu Verfahren der ITU /Xiph2011/, /Wiki2011/

Im Gegensatz zu den standardisierten und lizenzpflichtigen Verfahren der ITU stehen auch freie Verfahren, denen keine großen Standardisierungsorganisationen zugrunde liegen. Die Haltung der Entwickler gegenüber Standardisierungen und Lizenzen unterscheidet sich hier von Codec zu Codec, demzufolge gibt es welche, die auch einer Arbeitsgruppe der IETF unterliegen, andere unterliegen einer BSD-artigen Lizenz oder gehen aus einer Stiftung (Foundation) hervor.

Ein Nachteil von freien Verfahren ist, dass deren Standardisierung teilweise nicht strikt ist und es deshalb bei bestehenden Systemen im Zuge laufender Weiterentwicklung der Spezifikation teilweise zu Problemen in der Kompatibilität kommen kann.

Im Gegensatz dazu gibt es aber auch einige Vorteile. Die freie Entwicklungsstruktur, die hinter derartigen Verfahren steht, erlaubt den Einfluss einer breiten Schicht an Entwicklern, was darin resultiert, dass auf viele Bedürfnisse und Problemstellungen eingegangen werden kann.

Dazu gehört bei den hier behandelten Varianten beispielsweise die automatische Anpassung des Bandbreitenbedarfs und des Codierungsverfahrens an die Übertragungsverhältnisse. Steht genug Bandbreite für die Übertragung zur Verfügung, wird vom Verfahren dynamisch eine Codierungsvariante gewählt, die gute Qualität liefert. Bei weniger verfügbarer Bandbreite wird der Bandbreitenbedarf der Codierung kontrolliert verringert. Das hat zur Folge, dass selbst bei stark wechselnden Übertragungsbedingungen eine gute Sprachqualität erreicht werden kann. Aus diesem Grund finden diese Verfahren bei VoIP vorwiegend in mobilen Endgeräten oder Internetverbindungen ohne garantierte Bandbreite Verwendung.

Beispiele für weit verbreitete Codecs dieser Kategorie sind: /Wiki2011/

- Der freie Codec Speex geht aus einer Entwicklung der Xiph.Org Foundation hervor. Für die Übertragung werden 2 bis 44 kbit/s an Bandbreite benötigt, die Abtastraten können bei guten Bedingungen auf bis zu 48 KHz erhöht werden. Als Grundlage für dieses Verfahren dient CELP, ähnlich wie bei G.729.

- Mit „Silk“ hat der Hersteller Skype Technologies S.A. einen ebenfalls weit verbreiteten Codec im Einsatz. Im Gegensatz zu Speex ist Silk ursprünglich kein freier Codec, wurde aber dennoch 2009 standardisiert und freigegeben. Die benötigte Bandbreite liegt bei einer Abtastrate von bis zu 24 KHz bei 6 bis 40 kbit/s.

Tabelle 1-1 zeigt einen Überblick über einige der oben aufgeführten Codecs und deren Klassifizierung nach den im vorigen Abschnitt behandelten Kriterien.

Codec	Datenrate	Bitrate in kbit/s	Abtastrate	Codierung	MOS
G.711	fest	64	8 KHz	Abtastwert	4,4
G.729	fest	8	8 KHz	Segment	3,9
Speex	dynamisch	2 bis 44	8 bis 48 KHz	Segment	3,4-5,7

Tabelle 1-1: Eigenschaften ausgewählter Codecs /Fischer2008/

1.6 Real-Time Transport Protocol (RTP) /Badach2007/

Die Übertragung der Sprachpakete erfolgt in Echtzeit und hat somit spezielle Anforderungen an ein IP-Netz. Das verwendete Protokoll, das diesen Anforderungen nachkommen kann, ist das Real-Time Transport Protocol (RTP).

Zu den realisierten Funktionen zählen:

- **Garantie der Reihenfolge von RTP-Paketen**

  Durch eine Nummerierung der Pakete mit Sequenznummern kann deren korrekte Reihenfolge auf der Empfängerseite wieder hergestellt werden, falls sie auf dem Übertragungsweg verändert wurde.

- **Garantie der Isochronität**

  Ein Zeitstempel in jedem Paket erlaubt es dem Empfänger, dieselben Zeitabstände zwischen den Paketen herzustellen, wie sie zwischen den Paketen beim Absender waren. Die Isochronität der Daten wird damit garantiert.

Weitere Funktionen von RTP sind die Berücksichtigung von verschiedenen Quellen wie Audio, Video oder andere Echtzeitdaten. Außerdem bietet RTP Funktionen, die den Einsatz von Translatoren und Mixern erlauben. /Badach2007/

Ein RTP-Paket kann den wie in **Abbildung 1-6** dargestellten Aufbau haben:

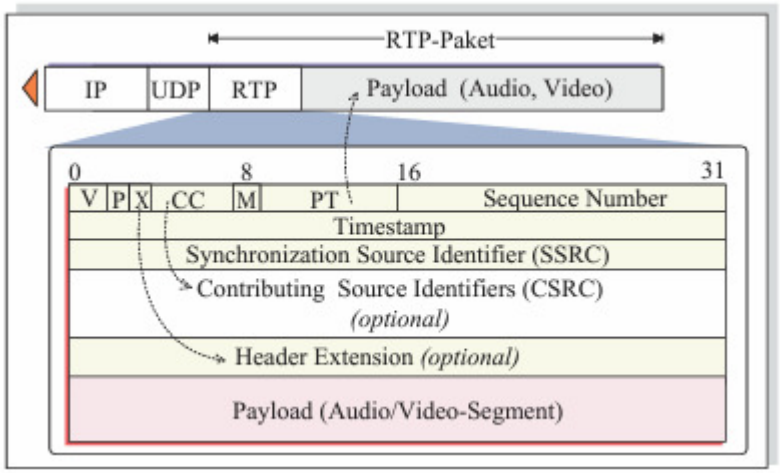


Abbildung 1-6: Aufbau eines RTP-Pakets /Badach2007/, S.153

Für eine typische Sprachübertragung entfallen die optionalen Header Contributing Source Identifiers (CSRC) und Header Extension, weshalb der RTP-Header in Summe 12 Byte ergibt. Darin sind als wichtige Bestandteile die Sequenznummer zur Herstellung der richtigen Reihenfolge, der Zeitstempel zur Garantie der Isochronität und der Synchronisation Source Identifier (SSRC) zur Identifikation der Quelle enthalten. Der SSRC-Header ist von Relevanz, wenn von einer Quelle mehrere RTP-Ströme stammen (Audio, Video).

Bei der Verwendung von Ethernet und weiteren notwendigen Protokollen aus dem TCP/IP-Protokollstack wie dem Internet Protocol (IP) und dem User Datagram Protocol (UDP) ergibt sich ohne die RTP-Header-Kompression die in **Abbildung 1-7** dargestellte Zusammenstellung eines Pakets für die Übertragung.

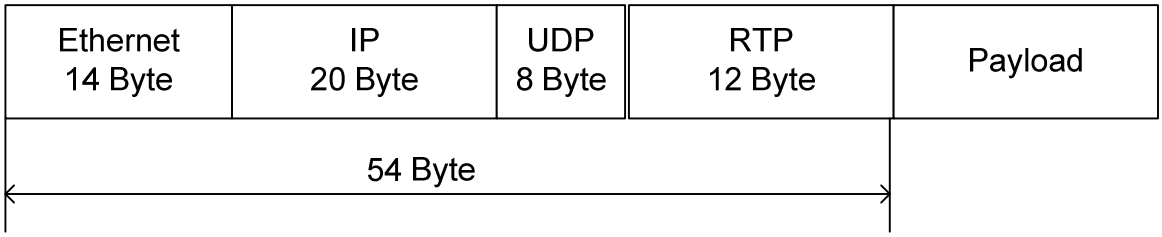


Abbildung 1-7: Zusammensetzung eines typischen RTP-Pakets

1.7 Real-Time Control Protocol (RTCP) /Badach2007/

Informationen, die Auskunft über die Gesprächsqualität während der Laufzeit eines Gesprächs geben, können mit RTCP gewonnen werden. Hierzu ist der periodische Austausch sogenannter Sender- und Receiver-Reports zwischen Sender und Empfänger geeignet.

Der Sender-Report (SR) wird dabei verwendet, um die Qualität der Übertragung aus der Sicht des Senders zu beschreiben. Beispielsweise wird hier dem Empfänger die Datenrate des Codecs mitgeteilt, um Überlastsituationen zu vermeiden.

Die Qualität des RTP-Stroms selbst kann mit dem Receiver-Report (RR) ermittelt werden, der die geschätzten Werte für Jitter, Delay oder Packet Loss übermittelt.

Pakete vom Typ SDES (Souce Description) enthalten einige Informationen über den Absender, wie Namen und Bezeichnungen, um verschiedene RTP- Ströme voneinander trennen zu können.

Mehrere dieser Pakete können in einem einzigen IP-Paket zusammengefasst werden, wenn das erforderlich ist.

1.7.1 Abschätzung des Jitter

RTCP verwendet bei der Berechnung von Jitter einfache Verfahren. Da jedes RTCP-Paket mit einem Zeitstempel versehen ist, ergibt sich die Verzögerung des Pakets beim Verlauf durch das Netz aus der Differenz zwischen Empfangszeitpunkt und Zeitstempel. Der momentane Jitter-Wert berechnet sich aus der Differenz zwischen den gemessenen Verzögerungen:

$Verzögerung_n = t_{Empfang} - t_{Zeitstempel}$

$Jitter = Verzögerung_n - Verzögerung_{n-1}$

1.7.2 Abschätzung der Round Trip Time (RTT)

Um den Wert für die Verzögerung für den Hin- und Rückweg eines Pakets abschätzen zu können, wird die Round Trip Time (RTT) verwendet. Die RTT ergibt sich aus der Summe der Verzögerung von Sender zu Ziel und jener von Ziel zu Sender.

Für die Berechnung ist somit jeweils ein RTCP-Paket pro Richtung erforderlich. Die Ermittlung der einzelnen Verzögerungen erfolgt analog zur Abschätzung des Jitter.

$$RTT = Verzögerung_{Quelle-Ziel} + Verzögerung_{Ziel-Quelle}$$

1.8 Skalen zur Darstellung von Gesprächsqualität

Unabhängig von den verwendeten Übertragungssystemen existieren mehrere Kennwerte, um die Gesprächsqualität einer Ende-zu-Ende-Übertragung auf einer Skala als einfachen Wert darzustellen. Auf die wichtigsten Varianten soll in diesem Kapitel eingegangen werden.

1.8.1 Mean Opinion Score (MOS)

Der MOS-Wert stellt die Qualität eines Gesprächs auf einer Skala zwischen 1 (schlecht) und 5 (sehr gut) dar. Die Ermittlung von MOS ist unabhängig von Werten wie Delay, Jitter und Packet Loss und erfolgt in einem standardisierten Testaufbau der die Voraussetzungen eines Testraums, der Endgeräte und der Testpersonen stellt. Die genaue Prozedur ist im Standard ITU-T P.800 beschrieben. **Tabelle 1-1** stellt die möglichen Werte dar, die von Testprobanden gewählt werden können und in **Tabelle 1-2** werden MOS-Werte von einigen verbreiteten Codecs unter idealen Laborbedingungen dargestellt.

MOS-Wert	Bedeutung
5 = excellent	keinerlei Anstrengung zum Verständnis der Sprache notwendig; totale Entspannung möglich
4 = good	keine Anstrengung notwendig, Aufmerksamkeit nötig
3 = fair	leichte, moderate Anstrengung nötig
2 = poor	merkbare, deutliche Anstrengung nötig
1 = bad	trotz Anstrengung keine Verständigung

Tabelle 1-1: MOS-Skala /Badach2007/, S.147

Verfahren	Bitrate [kbit/s]	MOS-Wert
PCM	64	4.3 - 4.5
ADPCM	16/24/32/40	3.4/3.6/3.9/4.2
CS-ACELP	8/6.4	4.0/3.8
LD-CELP	16	4.0 - 4.1
ACELP	5.3	3.5
MP-MLQ	6.3	3.7

Tabelle 1-2: MOS-Werte von Verfahren zur Sprachcodierung /Badach2007/, S.148

1.8.2 R-Faktor /Fischer2008/

Zur Bewertung kann auch der R-Faktor hinzugezogen werden. Dieser wird als Wert zwischen 0 (schlecht) und 120 (sehr gut) dargestellt, wobei der Wert typischerweise zwischen 50 und 90 in realen Netzen liegt. Nach der Definition im Standard G.107 wird für die Berechnung das sogenannte E-Modell verwendet. Es existiert ein (nichtlinearer) Zusammenhang zwischen dem R-Faktor und dem entsprechenden MOS-Wert, der beispielsweise von Tabellen entnommen werden kann.

Beispiele:

R-Faktor: 90 bis 50 entspricht

MOS: 4,34 bis 2,58

Im Gegensatz zum MOS-Wert lässt sich der R-Faktor nach einem mathematischen Modell berechnen:

$R = R_0 – I_S – I_d – I_{e\text{-}eff} + A$

Die genaue Einflussnahme der einzelnen Formelbestandteile auf R ist in G.107 definiert.

Die Auswirkung von verschiedenen zu berücksichtigenden Einflüssen wird wie folgt in der Formel berücksichtigt:

R_0… Basiswert der Signalstärke

repräsentiert Beeinflussung durch:
Umgebungsgeräusche, Raumgeräusche, Rauschen der Verbindung

I_s… Abschwächungswert für systembedingte Einwirkungen

repräsentiert Beeinflussung durch:
das klassische Netzwerk oder das IP-Netzwerk

I_D… Abschwächungswert für dynamisch funktionale Einwirkungen

repräsentiert Beeinflussung durch:
Echo des Senders, Echo beim Empfänger, absolute Laufzeitverzögerung

$I_{e\text{-}eff}$ … Abschwächungswert für elementare und effektive Einwirkungen

repräsentiert Beeinflussung durch:
Codecs mit niedrigeren Bitraten, Paket- oder Zellenverluste, Kontinuitätsfaktoren

A … Gewinnfaktor

symbolisiert den Einfluss der verwendeten Kommunikationsinfrastruktur

Für die genaue Berechnung des Wertes sind in G.107 und entsprechender Literatur Formeln und Tabellen vorgegeben. Die Tabellen basieren auf Erfahrungswerten und stellen zum Beispiel den Einfluss von verwendeten Codecs bei bestimmten Paketgrößen auf den $I_{e\text{-}eff}$-Wert dar.

Dynamisch veränderbare Werte wie Paketverlust oder Laufzeitverzögerung sind mithilfe einer weiteren Formel in die Berechnung mit einzubeziehen, um die endgültigen Werte für I_D und $I_{e\text{-}eff}$ zu erhalten. Der Gewinnfaktor A korrigiert das Ergebnis, um einen entsprechenden Wert nach oben, wenn mobile Kommunikationssysteme verwendet werden.

Für eine genauere Darstellung der Einfluss nehmenden Faktoren sei auf die Standards G.107 und G.113 verwiesen.

1.8.3 Bewertung der Skalen

Die MOS-Skala nach P.800 ist geeignet, um die Qualität eines bereits untersuchten Codecs zu beurteilen, wäre aber zu aufwändig, um ein laufendes System, das ständig unter dynamischen Einflüssen steht, zu analysieren.

Dennoch ist die MOS-Skala ein wichtiger Bezugswert, da die Darstellung einfach und leicht verständlich ist. Viele andere Verfahren erlauben eine Umrechnung in einen entsprechenden MOS-Wert, um einen direkten Vergleich zu erlauben.

Die Berechnung von MOS-Werten in einem laufenden System kann nicht exakt geschehen, aber mittels Schätzungen angenähert werden.

Das E-Modell und der R-Faktor können zur Beurteilung von herkömmlichen Telekommunikationssystemen oder auch IP-Netzen verwendet werden. Das Ergebnis der Berechnungen ist der R-Faktor.

Vorteile des E-Modells:

- Das E-Modell sieht einen breiteren Bereich für den Ergebniswert vor (0-120) als MOS (1-5), wobei der real zu erreichende Wert in modernen Netzen meistens kaum über 90 liegt. Dadurch ergibt sich mehr Raum für Verbesserung, falls heutige Technologien übertroffen werden können (z.B. durch die Anwendung von Wideband-Codecs).

- Alle Ausgangswerte können rechnerisch oder durch Tabellen ermittelt werden. Dadurch entsteht der Vorteil, dass keine Testpersonen, wie bei einer herkömmlichen Ermittlung von MOS, notwendig sind.

Vorteile von MOS:

- Die MOS-Skala ist die üblichere und weiter verbreitete Variante. Die Umrechnung des R-Faktors in einen MOS-Wert wird durch den nichtlinearen Zusammenhang erschwert.

- Die Ermittlung aller Ausgangswerte zur Berechnung des R-Faktors ist mit hohem Aufwand verbunden. Einige Werte müssen messtechnisch erfasst werden, um einen aussagekräftigen Wert für R zu erhalten. Besonders die messtechnische Erfassung von Paketverlusten, Verzögerungszeiten und Burstfehlern erweist sich, je nach Umgebung, als aufwändig und schwierig. Der MOS-Wert ist daher als Bezugswert sinnvoll.

2 Einflüsse der Übertragung über IP auf die Gesprächsqualität

Es bestehen viele Zusammenhänge zwischen Gesprächsqualität und Größen, die von der Übertragung über IP und nicht direkt von der analogen Signalverarbeitung in Endgeräten oder Codierungsverfahren herrühren. In diesem Abschnitt werden die verschiedenen möglichen Auswirkungen von IP-Netzen auf die Qualität untersucht.

In diese Betrachtung fallen nicht nur direkte Einwirkungen der Übertragungsmedien auf die übertragenen Daten, sondern auch Wechselwirkungen, die aufgrund des Bandbreitenbedarfs verschiedener Codecs und deren Parameter entstehen. Genaue Kenntnis über den Bandbreitenbedarf eines Codecs samt Protokolloverhead ist dann wichtig, wenn Gespräche über eine WAN-Strecke (Wide Area Network) gesendet werden und ein bestimmter Gesamtbedarf an Bandbreite nicht überschritten werden darf.

Für eine realistische Abschätzung der Einflüsse von IP-Netzwerken auf die Sprachübertragung ist die Betrachtung folgender Teilbereiche notwendig:

- indirekte und organisatorische Einflüsse auf die Qualität, die aufgrund des Bandbreitenbedarfs oder anderer Gegebenheiten entstehen
- direkte Einflüsse der Netze auf die Übertragung wie Delay, Jitter oder Paketverlust
- Einflüsse durch die Integration der IP-basierten Dienste in Endgeräten

Abbildung 2-1 veranschaulicht alle wesentlichen, auf die Qualität Einfluss nehmenden Größen und deren Standort im Netzwerk.

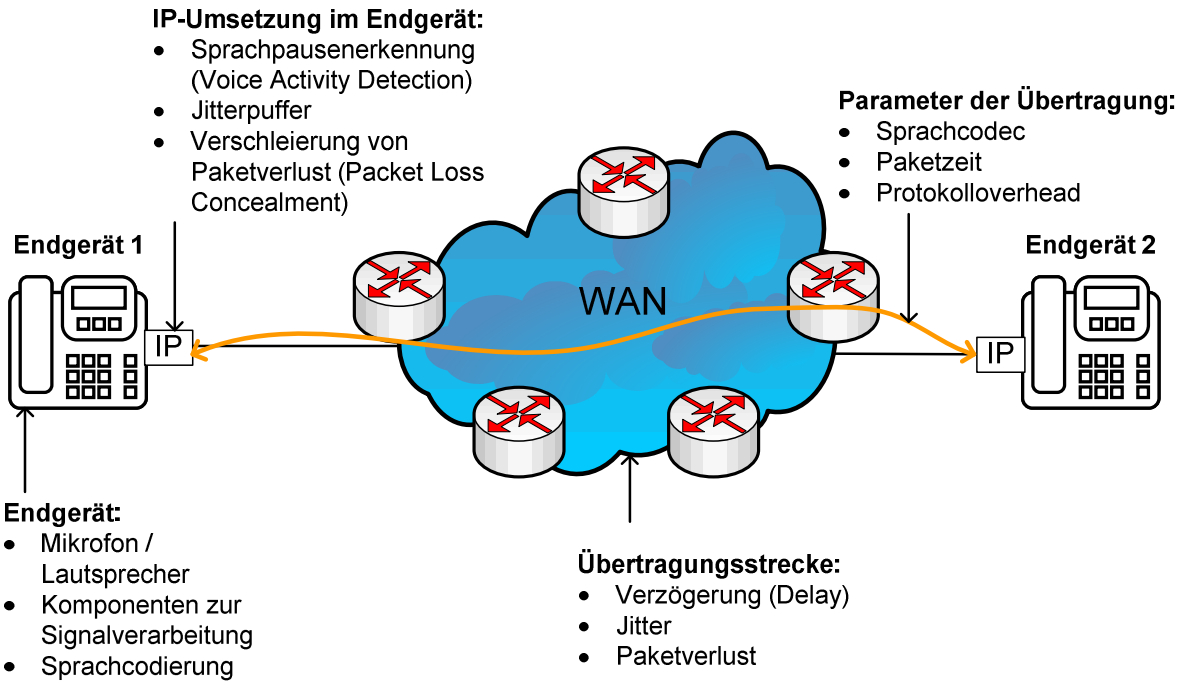


Abbildung 2-1: Mögliche Einflüsse auf Qualität bei VoIP

2.1 Organisatorische Einflüsse

In die Betrachtung der organisatorischen Einflüsse auf die Qualität fallen alle Parameter, die der Kontrolle der Techniker unterliegen und bei der Implementierung einer PBX richtig gewählt werden müssen. Dazu gehört beispielsweise die realistische Abschätzung des Bandbreitenbedarfs pro Gespräch. Eine falsche Einschätzung des Bedarfs über eine WAN-Übertragungsstrecke hat möglicherweise eine Überbuchung und Belastung der Strecke über das kalkulierte Maß hinaus zur Folge. Mögliche Auswirkungen sind ein Anstieg von Delay, Jitter oder Paketverlust und Einbußen bei der Übertragungsqualität.

2.1.1 Bildung von IP-Paketen

Nach der Anwendung von Codierungsverfahren müssen die Gesprächsdaten zur weiteren Verarbeitung im IP-Netz in Paketen zusammengefasst werden. Die Größe der Pakete, die darin enthaltenen Abtastwerte und damit die Dauer der wiedergegebenen Sprache können variieren. Die Methoden der Paketbildung haben Einfluss auf die Paketgröße und Paketanzahl und bestimmen den Bedarf der benötigten Bandbreite einer Übertragung.

2.1.2 Paketzeit (Packet Time)

Die Dauer eines Sprachfragments, das in einem Paket enthalten ist, liegt üblicherweise zwischen 10 ms und 60 ms und wird auch als Paketzeit, Packet Time oder ptime bezeichnet.

Die Wahl des genauen Wertes in der Implementierung hängt von bestimmten Erfordernissen ab, die aus den Qualitätsanforderungen und den Gegebenheiten im Netzwerk entstehen.

Die Wahl eines größeren Wertes anstelle eines kleineren bringt folgende Änderungen des Übertragungsverhaltens:

- eine Erhöhung der Ende-zu-Ende-Verzögerung des Audiosignals von „Mund zu Ohr“, die mindestens den Wert der Paketzeit annimmt, sich in der Praxis, je nach implementierten Jitter-Puffer, auch im doppelten Ausmaß oder mehr darauf auswirken kann. Die Folge dessen ist eine Verringerung der empfundenen Qualität.

- eine Verringerung der in Summe für die Übertragung benötigten Bandbreite, da weniger übertragene Pakete weniger Zusatzdaten für Übertragungsprotokolle (Protokolloverhead) zur Folge haben.

2.1.3 Auswirkungen der Paketbildung auf die Bandbreite

In diesem Abschnitt werden die Auswirkungen der Verfahren zur Paketbildung der Daten auf die Übertragungsbandbreite genauer untersucht. Dabei werden als untersuchte Codecs G.711 und G.729 verwendet. Das Codierungsverfahren von G.711 erzeugt 64 KBit/s, G.729 nur 8 KBit/s an Bitrate.

Die tatsächlich verbrauchte Bandbreite auf dem Übertragungsweg übersteigt dieses Maß aufgrund des vorliegenden Protokolloverheads pro Paket, der bei kleiner Paketzeit im Vergleich zur Nutzlast stärker ins Gewicht fällt als bei großer.

Die Grundlage für die Betrachtung des Bandbreitenbedarfs ist dabei eine messtechnische Untersuchung, bei der die Paketgröße bei gegebener Paketzeit ermittelt wurde, mit dem Ziel, die insgesamt benötigte Bandbreite zu ermitteln.

Mit entsprechenden Methoden der Netzwerkanalyse kann von einem beliebigen Datenstrom, wie einem Gespräch über VoIP, eine Aufzeichnung gemacht werden. Zu diesem Zweck wird hier die freie Software Wireshark verwendet. Damit ist es möglich, sofern das Netzwerk die erforderlichen Rahmenbedingungen bietet, den gesamten Netzwerkverkehr, der von einem Endgerät ausgeht, aufzunehmen und zu speichern.

Die Miteinberechnung aller Bestandteile des Protokolloverheads der Sprachübertragung, auch jene, die zwangsweise durch die asynchrone Übertragung im Netzwerk entstehen, ist aus folgenden Gründen sinnvoll:

- Der Ergebniswert eignet sich, um den Bandbreitenbedarf eines Gesprächs über eine Übertragungsstrecke realistisch einzuschätzen.

- Des Weiteren kann er, bei gegebener maximal verfügbarer Bandbreite einer Teilverbindung, zur Berechnung der Anzahl der maximal über die Strecke zu führenden Gespräche hinzugezogen werden.

- Der Einfluss des verwendeten Codecs, der Paketzeit und der Übertragungsprotokolle unter realen Bedingungen liegt bei einem Ausmaß, das deren Berücksichtigung notwendig macht. Die hohe Relevanz bei VoIP rührt auch von den hier verwendeten, kleinen Paketen her, die den Protokolloverhead stärker ins Gewicht fallen lassen.

Der Wert von 54 Bytes für den Protokolloverhead, wie er in **Abbildung 1-7** gezeigt wird, entspricht jenem, der mit Wireshark gemessen werden kann und von jedem Gerät im Netzwerk wahrnehmbar ist. Durch die für IP-Netze übliche asynchrone Übertragung entstehen zwangsläufig Pausen zwischen den Übertragungen, die auch als Overhead berücksichtigt werden müssen.

Unter idealen Bedingungen bei Ethernet fallen die pro Paket zu berücksichtigenden Werte für Fehlerkorrektur (Cycling Redundancy Check 32 – CRC32), die notwendige Lücke zwischen den Paketen (Inter Frame Gap – IFG) und das Präambel mit Begrenzungssymbol (Start of Frame Delimiter – SFD) an, wie in **Tabelle 2-1** aufgeführt wird. Die hier dargestellten Werte spiegeln die Bedingungen einer typischen Übertragung in einem lokalen Netzwerk, basierend auf Ethernet, wider.

Protokoll	**Bedarf/Byte**
Ethernet	14
CRC32	4
IFG	12
Präambel, SFD	8
IP	20
UDP	8
RTP	12
Summe	**78**

Tabelle 2-1: Bestandteile des Protokolloverheads

An dieser Stelle ist anzumerken, dass die Übertragung mittels Ethernet eine Methode bei VoIP darstellt, die einen vergleichsweise geringen Protokolloverhead zur Folge hat. Bei der Verwendung von kabellosen Netzen wie WLANs oder UMTS oder bei Benutzung von

virtuellen privaten Netzwerken (VPNs) oder Multiprotocol Label Switching (MPLS) erhöht sich der Overhead teilweise beträchtlich.

Die Aufzeichnungen von Gesprächen, die mit G.711 oder G.729 codiert sind, ergeben bei verschiedenen Paketzeiten von 20 ms, 30 ms oder 60 ms die in **Tabelle 2-2** dargestellten Paketgrößen in Bytes. Die für die Bandbreitenberechnung hinzuzuziehende reale Paketgröße unterscheidet sich von der gemessenen insofern, dass hier 24 Bytes zusätzlich für CRC32, IFG und SFD für die Bedingungen im lokalen Netz berücksichtigt worden sind.

Aus den gemessenen Werten kann mit folgender Formel der tatsächliche Bandbreitenbedarf errechnet werden:

$$\text{Bandbreite(kbps)} := \frac{\text{Paketgröße}}{\text{Paketzeit}} \cdot 8$$

Weiters ergibt sich der prozentuale Protokolloverhead aus dem Vergleich der real benötigten Bandbreite mit der für die Codierung benötigten Bandbreite, was den Nutzdaten entspricht:

$$\text{Protokolloverhead(\%)} := 100 \cdot \left(\frac{\text{Bandbreite}_{\text{Real}}}{\text{Bandbreite}_{\text{Nutzdaten}}} - 1 \right)$$

Codec	Paketzeit / ms	Paketgröße / Byte		Bandbreite / Kbit/s		Overhead(%)
		gemessen	real	Nutzdaten	real	
G.711	20	214	238	64	95,2	49%
	30	294	318	64	84,8	33%
	60	534	558	64	74,4	16%
G.729	20	74	98	8	39,2	390%
	30	84	108	8	28,8	260%
	60	114	138	8	18,4	130%

Tabelle 2-2: Paketgrößen und Bitraten bei Sprachcodierung

Eine grafische Darstellung der in **Tabelle 2-2** aufgeführten Messwerte ergibt den in **Abbildung 2-2** dargestellten nichtlinearen Zusammenhang zwischen der Paketzeit und der benötigten Bandbreite. Als Intervall der dargestellten Paketzeit wurde 10 ms bis 60 ms gewählt.

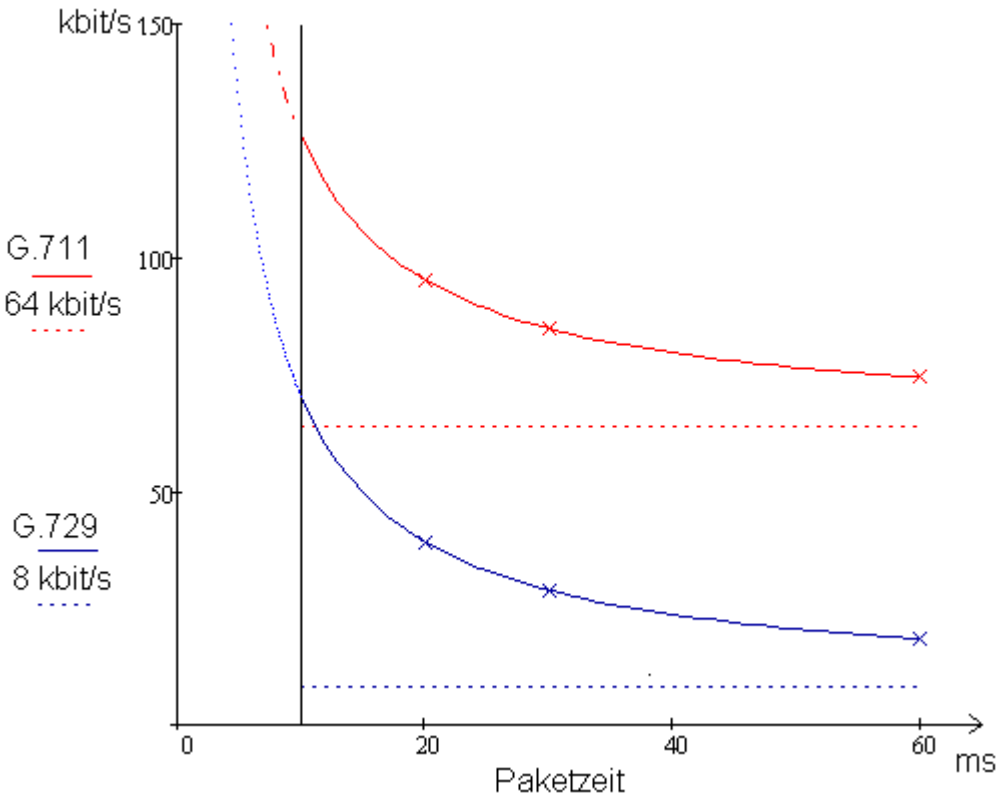


Abbildung 2-2: Bitraten von G.711 und G.729 bei variabler Paketzeit und konstantem Protokolloverhead

Aus der Untersuchung des Bandbreitenbedarfs der Codecs ergeben sich folgende Erkenntnisse:

- Bereits die Verwendung von kürzeren Paketzeiten als 20 ms hat einen sehr starken Anstieg des Overheads im Vergleich zur Nutzlast zur Folge.
- Bei der Verwendung von G.729 und 20 ms Paketzeit erreicht der Overhead bereits nahezu das vierfache Ausmaß der Nutzlast.
- Der vergleichsweise geringste Overhead wird hier mit G.711 und 60 ms erreicht und liegt bei 16%.

Bei der Wahl der Paketzeit sind die Anforderungen an die Qualität zu berücksichtigen, somit ist ein geeigneter Kompromiss zwischen Qualität und Bandbreitenbedarf zu finden. Diese Entscheidung kann beispielsweise aufgrund der nachfolgenden Zielsetzungen getroffen werden.

Zielsetzung 1: Es ist genug Bandbreite vorhanden und es soll maximale Qualität erreicht werden.

In diesem Fall ist beispielsweise G.711 mit 20 ms eine geeignete Wahl.

Zielsetzung 2: Die Bandbreite ist limitiert, es soll bei bestmöglicher Qualität so wenig Bandbreite wie möglich verbraucht werden.

Hier wäre die Wahl von G.729 mit 60 ms empfehlenswert.

2.2 Direkte Einwirkungen von IP-Netzen auf die Paketübertragung

Einige nicht ideale Eigenschaften der Übertragung von Paketdaten über IP-Netze haben maßgeblichen Einfluss auf die Qualität von VoIP. Die Ursachen hierfür sind vielfältig und unterscheiden sich je nach verwendeter Netzwerkinfrastruktur. Die Einflussfaktoren, mit denen die Auswirkungen auf VoIP messbar sind, werden in diesem Abschnitt behandelt.

2.2.1 Delay und Round Trip Time (RTT)

Die Ende-zu-Ende-Verzögerung von Paketen hat einen wesentlichen Einfluss auf die wahrgenommene Gesprächsqualität. Hierbei ist zwischen folgenden relevanten Darstellungsarten der Verzögerung zu unterscheiden:

- **Round Trip Time (RTT):**

Die Round Trip Time definiert die Summe der Verweildauer von Paketen im Netz in beide Richtungen einer Kommunikation.

$RTT = T_{SR} + T_{RS}$

T_{SR} ... Verzögerung von Endpunkt 1 (Sender) zu Endpunkt 2 (Empfänger)
T_{RS} ... Verzögerung von Endpunkt 2 (Empfänger) zu Endpunkt 1 (Sender)

Die RTT ist von Interesse, um Aussagen aufgrund eines einzelnen Kennwertes zu treffen, da es sich bei VoIP üblicherweise um eine 2-Wege-Kommunikation handelt.

- **Mouth-to-Ear-Delay (Mund-zu-Ohr-Verzögerung) T_{EE}:**

Dieser Kennwert definiert die gesamte Verzögerung der Sprache zwischen Sender und Empfänger, inklusive Codierungszeit.

T_{EE} ... Verzögerung von Endpunkt 1 (Sender) zu Endpunkt 2 (Empfänger)

$T_{EE} = T_{CP} + D_0 + t_{ü} + T_{JP}$ /Badach2007/

Definitionen der einzelnen Formelbestandteile:

- T_{CP} ... Codierungs- und Paketierungszeit = konstant
  $T_{CP} = T_{seg} + T_{Look\text{-}Ahead}$
  T_{seg} ... Dauer eines Gesprächssegments, auch ptime, typischerweise 20-60 ms
  $T_{Look\text{-}Ahead}$ ... reservierte Zeit für die Paketierung

- D_0 ... Serialisierungszeit

  D_0 = Paketgröße [Bit] / Übertragungsrate [Bit/s]

- $t_ü$ ... Übermittlungszeit

  → erhöht sich je nach Anzahl der Knoten zur Wegewahl des Pakets (Router)

  Bei einem Knoten zwischen Sender und Empfänger ergibt sich diese Zeit zu:

  $t_ü = T_0 + \tau_1 + D_1 + T_1$

  T_0 ... Übertragungszeit von IP-Telefon zu Router 1

  τ_1 ... zufällige Wartezeit in Router 1

  D_1 ... Serialisierung durch Router 1

  T_1 ... Übertragungszeit von Router 1 zu Router 2

- T_{JP} ... Zeit, die ein Paket im Jitter-Puffer (siehe **Abschnitt 2.3.1**) verbringt

T_{CP} kann als konstant angenommen werden, die Komponenten D_0 und T_{JP} sind implementierungsabhängig und sind für ein laufendes System kalkulierbar. Die Übertragungszeit $t_ü$ ist variabel und kann somit den größten Einfluss auf das System haben.

Je nach Anforderung, Implementierung und Endgerätetyp gilt ein T_{EE}-Wert von mehr als 150-300 ms als nicht mehr ideal. Richtlinien und Empfehlungen für die einzelnen Werte sind, wie in **Abbildung 2-3** dargestellt, im ITU-Standard G.114 definiert.

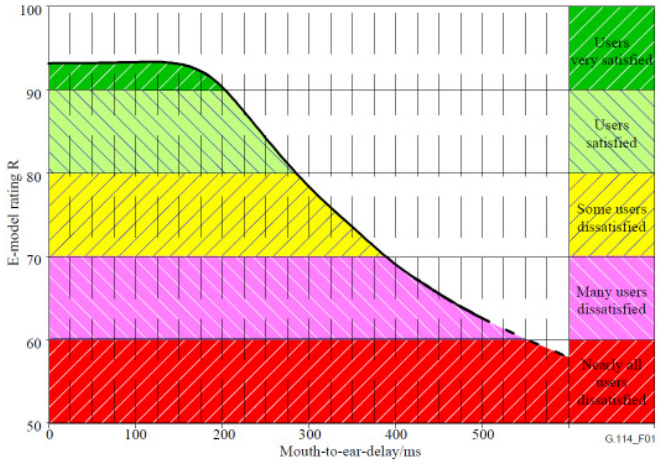


Abbildung 2-3: Zusammenhang zwischen T_{EE} und Qualität in G.114 /ITU11/, G.114, S.3

2.2.2 Laufzeitschwankungen (Jitter) /Fischer2008/

Bei der Kommunikation in einem IP-Netz ist es nötig, dass die Zeitabstände zwischen den Paketen auf der Sende- und Empfangsseite unverändert bleiben. Die gleichbleibende zeitliche Verzögerung wird Isochronität genannt. Eine der Anforderungen an das Netz ist

es daher, diese sicherzustellen. Durch Laufzeitschwankungen, bedingt durch verschiedene Wegewahl, unterschiedliche Latenzen und andere Einflüsse, ist in einer realen Umgebung mit einem nicht isochronem Datenstrom zu rechnen, der mithilfe eines Jitter-Ausgleichpuffers wieder korrigiert werden muss. Auf die Anforderungen und die Möglichkeiten zur Realisierung eines Jitter-Puffers wird in **Abschnitt 2.3.1** genauer eingegangen.

2.2.3 Paketverlust (Packet Loss)

Eine wesentliche Beeinträchtigung entsteht durch den Verlust von Paketen auf der Übertragungsstrecke. Verlorene Pakete können auch durch Maßnahmen wie Jitter-Puffer nicht korrigiert werden. Diese werden auch vom Empfänger nicht wiederholt angefordert, da dieser Vorgang weitere (nicht akzeptable) Verzögerungen zur Folge hätte.

Der Einfluss des Verlustes von einzelnen Paketen bzw. Segmenten kann daher durch Generierung von Hintergrundrauschen anstelle des fehlenden Segments minimiert werden. Die Generierung dieses Segments funktioniert in verschiedenen Systemen, je nach Art der Implementierung, unterschiedlich gut. /Fischer2008/

Das Fehlen von vielen Segmenten führt, je nach deren Verteilung im Datenstrom, zu hohen Qualitätseinbußen, insbesondere, wenn viele aufeinanderfolgende Segmente fehlen (Burstfehler). Niedrige und deutlich verteilte Verlustraten können durch gut ausgleichende Methoden unbemerkt bleiben. Der Paketverlust kann hier in drei verschiedene Ausprägungen eingeteilt werden:

- **nominaler Paketverlust**

  → Anzahl der Summe der Pakete, die während einer Verbindung verloren gehen

- **prozentualer Paketverlust**

  → Prozentsatz der verlorenen Pakete im Vergleich zu den insgesamt übertragenen Paketen (Wert sollte 3-5 % nicht übersteigen)

- **Burstfehler**

  → Anzahl der Pakete, die hintereinander verloren gehen

2.2.3.1 Nominaler Paketverlust

Die Messung des nominalen Paketverlustes erlaubt es noch nicht, Aussagen über die Gesprächsqualität zu treffen. Unter Berücksichtigung der Gesprächsdauer lässt sich daraus der prozentuale Paketverlust errechnen, der für eine Beurteilung der Gesprächsqualität geeignet ist. Der Wert, der von RTCP geliefert wird, entspricht dem nominalen Paketverlust.

2.2.3.2 Prozentualer Paketverlust

Die Formel zur Errechnung des prozentualen Paketverlusts lautet:

$$PL_P := \frac{PL_N}{Anzahl_{PaketeGesamt}} \cdot 100\%$$

PL_P ... prozentualer Paketverlust

PL_N ... nominaler Paketverlust

Unter der Bedingung, dass ein übertragenes Segment einem Paket entspricht, kann für die Berechnung die Zeit des Sprachdatenstroms herangezogen werden:

$$PL_P = PL_N * \frac{T_{seg}}{T_{call}}$$

T_{call} ... analysierter Zeitraum des Sprachdatenstroms

T_{seg} ... Dauer eines Gesprächssegments

Bei gleichmäßiger Verteilung der Fehler in einem Beobachtungszeitraum bzw. bei gleichbleibenden Übertragungsverhältnissen ist der prozentuale Paketverlust ein geeignetes und aussagekräftiges Mittel zur Analyse.

2.2.3.3 Burstfehler

Die Menge und die Länge der Burstfehler können ebenfalls für die Auswertung von Interesse sein. Mit der Analyse der Burstfehler lassen sich Aussagen über die Verteilung der Paketverluste auf den Datenstrom treffen.

Von Interesse ist hier die Anzahl der Pakete, die aufgrund eines Burstfehlers verloren gegangen sind:

PL_B ... Anzahl aufeinanderfolgender verlorener Pakete

Ab welcher Anzahl an aufeinanderfolgenden verlorenen Paketen kann man anstelle von einfachem Paketverlust von Burstfehlern sprechen?

Diese Grenze ist nicht eindeutig definiert, jedoch kann als Vergleichswert hierfür das Verhältnis zwischen nominalem Paketverlust und verlorenen Paketen innerhalb eines Bursts herangezogen werden:

$PL_{PB} = PL_B / PL_N$

Ist das Verhältnis eher hoch bzw. beträgt es nahezu 100 %, kann man von einem Burstfehler sprechen. Bei einem niedrigen Verhältnis kann angenommen werden, dass

keine Burstfehler vorhanden oder viele Burstfehler innerhalb des Beobachtungszeitraums aufgetreten sind. In diesem Fall kann der Zeitraum verringert werden. Dabei kann, je nach Sinnhaftigkeit, etwa bei einem Verlust von zwei aufeinanderfolgenden Paketen oder erst ab 100 Paketen, ein Fehlerfall als Burstfehler definiert werden.

Das bedeutet generell, dass ein analysierter Datenstrom zum Zeitpunkt eines Burstfehlers eine hohe Fehlerdichte im Vergleich zu einem fehlerfreien Betrieb aufweist.

Die Anzahl und die zeitliche Verteilung von Burstfehlern können Aufschluss über den Ursprung eines Problems geben. Wird ein Burstfehler durch eine ansteigende Dichte der Fehler erkannt, kann beispielsweise davon ausgegangen werden, dass es im IP-Netz zu einer Überlastungssituation gekommen ist. Die Verteilung der Fehler auf einzelne Endgeräte kann Aufschluss über die Lokation der betroffenen Teilstrecke geben.

Die Auswertung der Burstfehler ist geeignet für eine erweiterte Analyse bei ungleichmäßiger Verteilung der Paketverluste innerhalb eines Beobachtungszeitraums, da der prozentuale Paketverlust nicht die Verteilung der Fehler berücksichtigt.

2.3 Qualitätsunterschiede bei der Implementierung in Endgeräten

Es gibt Unterschiede bei den Implementierungen der IP-Funktionen in den Endgeräten, welche die Sprachübertragung über Netze auch beeinflussen. In diesem Abschnitt werden einige Größen behandelt, die bei Endgeräten verschiedener Hersteller und Qualität auf unterschiedliche Weise realisiert werden und deren Fähigkeit, mit Problemen im IP-Netz umzugehen, beeinflussen.

2.3.1 Jitter-Puffer

Dieser Teil eines Endgerätes bietet einen Zwischenspeicher im Endgerät, der Laufzeitunterschiede der Pakete (Jitter) ausgleichen kann.

Die Größe des Jitter-Puffers wird je nach erwarteten Jitter-Werten gewählt und muss abhängig vom verwendeten Codec ausreichend Speicherplatz vorsehen. Typische Werte für einen Jitter-Puffer liegen bei folgenden Größen:

$T_{seg} < T_{JP} < 2*T_{seg}$

T_{seg} ... Dauer eines Gesprächssegments

T_{JP} ... Jitter-Puffer-Zeit

Ein kleiner Puffer führt somit zu kleinen Latenzwerten, aber zu höheren Paketverlustraten; ein großer Puffer hat größere Latenzzeiten und kleinere Paketverlustraten zur Folge.

Die erhöhte Paketverlustrate resultiert bei kleinen Jitter-Puffern darin, dass Pakete, die „zu spät“ beim Empfänger ankommen, verworfen werden müssen.

Da sich sowohl hohe Latenzen als auch hohe Paketverlustraten negativ auf die Gesprächsqualität auswirken, muss bei der Größenwahl des Jitter-Puffers ein Kompromiss zwischen beiden Faktoren getroffen werden. **Abbildung 2-4** zeigt die Verteilung der Laufzeiten der Pakete und die Abhängigkeit der Paketverlustrate von der Dimensionierung des Jitter-Puffers.

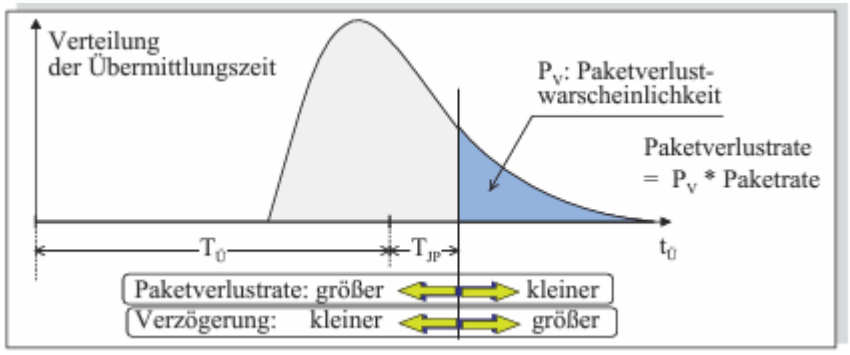


Abbildung 2-4: Jitter-Ausgleichpuffer und Paketverluste /Badach2007/

Die Dauer T_J definiert den Laufzeitunterschied eines Paketpaares.

Beispiel: T_{seg} = 30 ms

Paket 1 kommt zum Zeitpunkt T_a am Ziel an.
Paket 2 kommt zum Zeitpunkt T_a + 35 ms an.

Damit gibt es zwischen den Paketen einen Laufzeitunterschied von + 5 ms.

→ T_J = 5 ms

Bei der Erfassung von vielen Messpaaren lässt sich die durchschnittliche Jitter-Zeit errechnen oder eine Verteilungsfunktion darstellen.

Ein Jitter-Puffer sollte bei einer Sprachkommunikation über IP-Netze immer existieren, um gute Qualitätswerte zu sichern. Die Form der Implementierung kann sich unterscheiden. Die Dauer T_{JP} und damit die Größe des Jitter-Puffers können in einem System

- **konstant** nach vorher festgelegten Werten oder
- **dynamisch veränderbar** definiert sein (adaptiver Jitter-Puffer).

Ein konstanter Wert für T_{JP} hat den Vorteil einer einfachen Realisierung. Als Nachteil gilt aber eine gleichbleibende (hohe) Verzögerung, auch bei guten Übertragungsverhältnissen.

Darüber hinaus existiert die Möglichkeit einer zeitlich veränderbaren Größe des Jitter-Puffers je nach Übertragungsverhältnis. Steigt beispielsweise die Paketverlustrate durch äußere Einflüsse an, kann der Jitter-Puffer erhöht werden, um den Fehler auf Kosten der

Verzögerung zu korrigieren. Umgekehrt kann bei guten Übertragungsverhältnissen der Jitter-Puffer verringert werden, um niedrigere Verzögerungen zu erreichen.

Die Wahl der Implementierung ist einem Analysten des Systems oftmals nicht zugänglich, da diese in vielen Fällen von einem Hersteller nicht offen gelegt wird.

Für diesen ist hier abzuwägen, welche Art der Realisierung bei angemessenem Aufwand ein akzeptables Ergebnis erzielt.

In jedem Fall wirkt sich ein schlecht implementierter oder nicht vorhandener Jitter-Puffer negativ auf die Gesprächsqualität bei wechselnden Übertragungsverhältnissen aus.

Typische Werte für konstante Jitter-Puffer liegen, je nach Paketzeit, bei 30-50 ms, adaptive Puffer können diese Zeit auf 100-500 ms erhöhen, wobei bei einer Größe von über 100 ms Qualitätsprobleme durch die zu hohe Zeitverzögerung auftreten können.

2.3.2 Sprachpausenerkennung

Ein weiteres Merkmal der unterschiedlichen Integration von IP in Endgeräten ist die Sprachpausenerkennung, auch als Voice Activity Detection (VAD) bezeichnet.

Wenn dieses Leistungsmerkmal eingeschaltet ist, erkennt ein Endgerät eine Pause im Gespräch und lässt die Sprachcodierung und die Datenübertragung für diese Dauer entfallen.

Der Vorteil dieses Verfahrens ist ein entsprechendes Ersparnis beim Bandbreitenbedarf, wobei dessen Ausmaß von der Charakteristik des Gesprächs selbst abhängig ist.

Der Nachteil ist jedoch, dass die Sprachpausen, je nach Endgerätetyp, häufig durch Stille ersetzt werden, die von einem Zuhörer in der Regel als unnatürlich und unangenehm empfunden wird.

In aufwendigeren Implementierungen von Sprachpausenerkennung wird aus diesem Grund die Stille beim Empfänger durch Komfortrauschen (Comfort Noise) ersetzt, das, je nach Verfahren, dem natürlichen Hintergrundrauschen eines Gesprächs recht nahe kommen kann. Unterschiedliche Verfahren, die in den Endgeräten zur Anwendung kommen, liefern auch unterschiedlich gute Ergebnisse.

2.3.3 Maskierung von Paketverlust

Im Fall von Paketverlust müssen an einem Endgerät Maßnahmen getroffen werden, um fehlende Pakete im Datenstrom zu ersetzen. Die verschiedenen Verfahren, die hier angewandt werden können, haben zum Ziel, den aufgetretenen Paketverlust zu maskieren und werden auch als Packet Loss Concealment (PLC) bezeichnet. Dabei ist zwischen drei verschiedenen Lösungsansätzen zu unterscheiden:

- **Ersetzen durch Stille:**

  Bei diesem einfachen Verfahren werden fehlende Pakete durch Stille ersetzt. Das Ergebnis der Rekonstruktion ist mäßig, da sich Paketverlust durch deutlich wahrzunehmendes Krachen auswirkt.

- **Wiederholen des letzten empfangenen Pakets:**

  Dadurch werden zwar bessere Ergebnisse als beim ersten Verfahren erreicht, aber wenn mehrere Pakete hintereinander verloren gehen, ist der Qualitätsverlust trotzdem groß.

- **Verwendung prädiktiver Algorithmen:**

  Mit erweiterten Verfahren ist es möglich, aus mehreren vorangegangenen Paketen das verlorene durch Schätzungen zu rekonstruieren. Je nach Algorithmus ist das Ergebnis unterschiedlich gut, in der Regel ist es jedoch besser als bei den ersten beiden Verfahren.

3 Implementierung einer Lösung mit RTCP

Eine Möglichkeit, den Anforderungen an eine Überwachungslösung von Qualität bei VoIP Rechnung zu tragen, ist die Aufzeichnung von Qualitätsmerkmalen an einer zentralen Stelle, einem Server. Als Quelle der Kennwerte können die RTCP-Daten verwendet werden. Diese Werte müssen mit geeigneten Mitteln zum Server transportiert werden und dort archiviert sowie für den Systemadministrator bereitgestellt werden.

3.1 Anwendungsszenario von VoIP mit mehreren Lokationen

Die typische Anwendung von VoIP in einem Unternehmen besteht aus mehreren Standorten, bestehend aus einer Zentrale und beliebig vielen Filialen. Für gewöhnlich gibt es außer der Filiale noch einen zweiten Standort mit ähnlicher technischer Infrastruktur, die bei einem Ausfall der Zentrale alle Funktionen übernimmt.

Die Vernetzung der Standorte untereinander erfolgt in Form eines VPN, um die durchgängige Form der Kommunikation für VoIP zu ermöglichen. Das hat zur Folge, dass die Gespräche zwischen den Standorten nicht über das öffentliche Telefonnetz geführt werden und so keine zusätzlichen Telefongebühren entstehen.

Die Anforderungen an ein VPN können mit verschiedenen Mitteln erreicht werden. Eine Technologie, die hier breite Anwendung findet ist MPLS. Ein Vorteil davon ist, dass die Pakete eines Datenstroms, im Unterschied zu einer gewöhnlichen Übertragung über das Internet, im „Gänsemarsch“ übertragen werden und somit bessere Werte für RTT, Jitter und Packet Loss liefern, ohne zusätzlich QoS-Merkmale abbilden zu müssen.

Abbildung 3-1 illustriert ein solches Anwendungsszenario in einem Unternehmen.

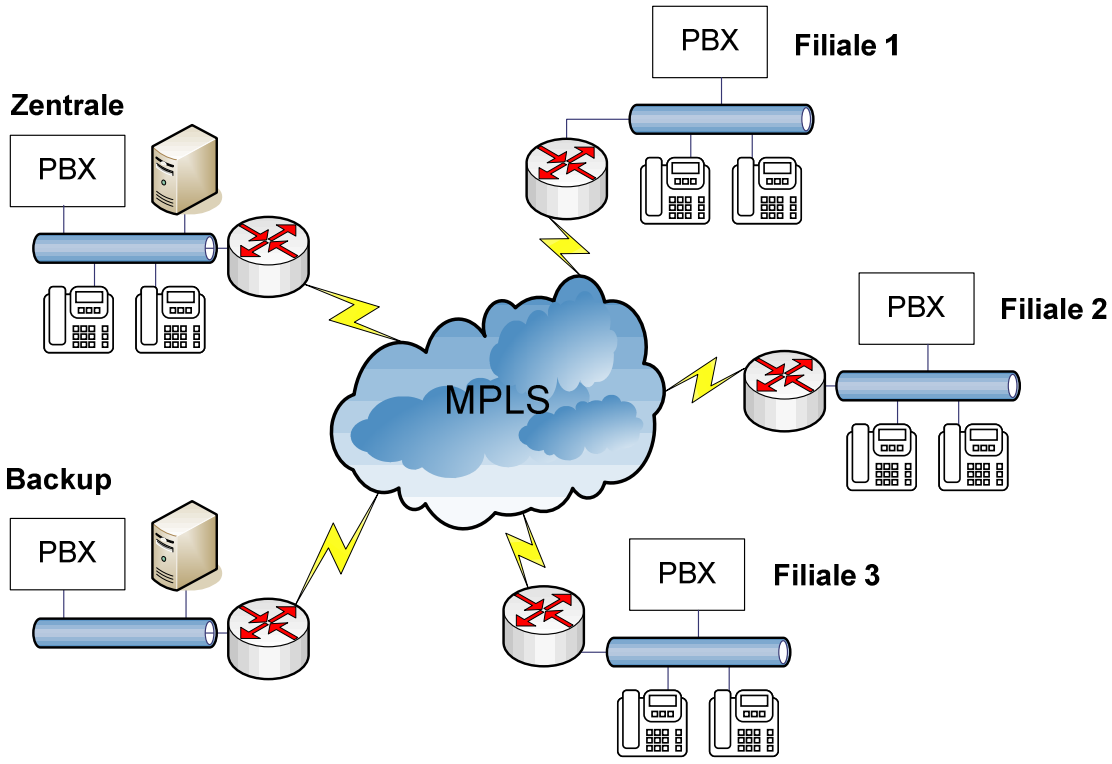


Abbildung 3-1: Anwendungsszenario von VoIP in einem Unternehmen

Als VoIP-Telefonanlagen sind PBXen vom Hersteller Innovaphone im Einsatz. In den folgenden Abschnitten wird von einer homogenen Umgebung mit Innovaphone-Komponenten als Endgeräte ausgegangen.

3.1.1 Aufbau der RTCP-Implementierung

Die Endgeräte verwenden für jede bestehende RTP-Sitzung das Protokoll RTCP, um die Qualität der Sitzung zu überwachen. Zu diesem Zweck werden in einem Zeitabstand von 10 Sekunden RTCP-Pakete zwischen Sender und Empfänger eines RTP-Stroms ausgetauscht. Die enthaltenen Informationen in einem Paket sind wie in **Abbildung 3-2** strukturiert. Als Grundlage für die Berechnung weiterer Kennwerte (RTT, Jitter, Paketverlust) zählen die Einträge „Cumulative number of packets lost“ (1), „Interarrival jitter“ (2) und „Delay since last SR timestamp“ (3).

```
⊟ Source 1
    Identifier: 0xda8c69e9 (3666635241)
  ⊟ SSRC contents
      Fraction lost: 0 / 256
      Cumulative number of packets lost: 0 <-- (1)
  ⊟ Extended highest sequence number received: 51909
      Sequence number cycles count: 0
      Highest sequence number received: 51909
    Interarrival jitter: 0 <-- (2)
    Last SR timestamp: 1967267 (0x001e04a3)
    Delay since last SR timestamp: 654417 (9985 milliseconds) <-- (3)
```

Abbildung 3-2: Auszug aus Wireshark-Trace von RTCP

Die Frequenz, mit der RTCP-Daten ausgetauscht werden, ist mit 1 Paket pro 10 s in dieser Implementierung konstant. Der Austausch der RTCP-Daten erfolgt zwischen allen Endgeräten, die bei einer Kommunikation beteiligt sind. Diese Möglichkeit besteht zwischen zwei VoIP-Endgeräten und zwischen Endgerät und PBX. Alle Funktionen, welche diese Implementierung von RTCP bietet, können zunächst nur verlässlich realisiert werden, wenn die verwendeten Komponenten vom selben Hersteller sind. Bei den Komponenten von Innovaphone sind die Pakete als Sender Report (SR) mit Source Description (SDES) realisiert. In **Abbildung 3-3** werden diese Basisszenarien illustriert. Der Ablauf ist automatisiert und bedarf keiner zusätzlichen Konfiguration.

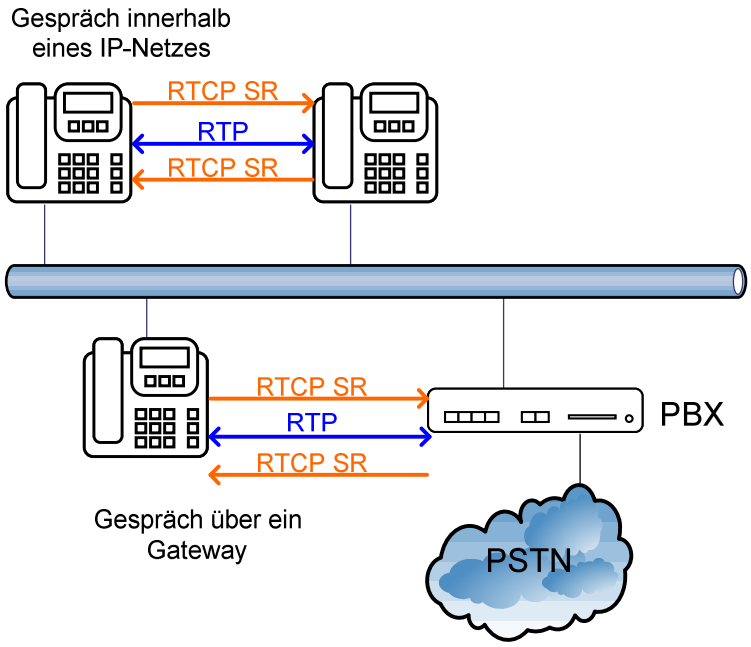


Abbildung 3-3: Basisszenarien bei der Anwendung von RTCP SR / SDES

Die Software der Endgeräte und der PBX nimmt die weitere Berechnung der Werte für RTT, Jitter und Packet Loss vor. Die Ergebnisse der Berechnungen sind:

- die durchschnittliche RTT für die Dauer des gesamten Gesprächs
- die momentane RTT

- der durchschnittliche Jitter-Wert für die Dauer des ganzen Gesprächs
- der momentane Jitter-Wert
- die Summe der verlorenen Pakete für die Dauer des gesamten Gesprächs

Alle Kennwerte können als eine durch ein Zeichen, zum Beispiel „+“, getrennte Zahlenfolge dargestellt werden:

15+15+7+7+0

In diesem Beispiel betragen der momentane sowie der durchschnittliche Wert für RTT 15 ms, für Jitter 7 ms. Diese (nicht standardisierte) Darstellungsweise findet bei Innovaphone in den Syslog-Meldungen Anwendung.

In die hier dargestellte Berechnung für RTT fließt nur die Verzögerung ein, die aufgrund der Eigenschaften des Netzwerks entsteht. Codierungs-, Serialisierungs-, und Jitter-Puffer-Zeiten werden nicht berücksichtigt, da sie für die Übertragung als konstant angenommen werden können. (vgl. **Abschnitt 2.2.1**)

3.1.2 Serverbasierende Erfassung von RTCP-Daten

Je nach verwendeten Komponenten gibt es einige Möglichkeiten, die RTCP-Kennwerte auf einem Server zu erfassen. Das Sammeln dieser Daten an einer zentralen Stelle hat den Vorteil, dass sie anschließend von diesem zentralen Punkt zur Verfügung gestellt werden können. Dabei können, wie in **Abbildung 3-4** dargestellt, beliebig viele PBXen und Endgeräte als Quellen der RTCP-Daten dienen. Zur Übertragung der Daten zum Server wird nicht RTCP verwendet, sondern das Protokoll Syslog. Hierzu werden die RTCP-Daten von jeder PBX in Form eines Call Detail Records (CDR) in eine Syslog-Meldung verpackt und gesendet.

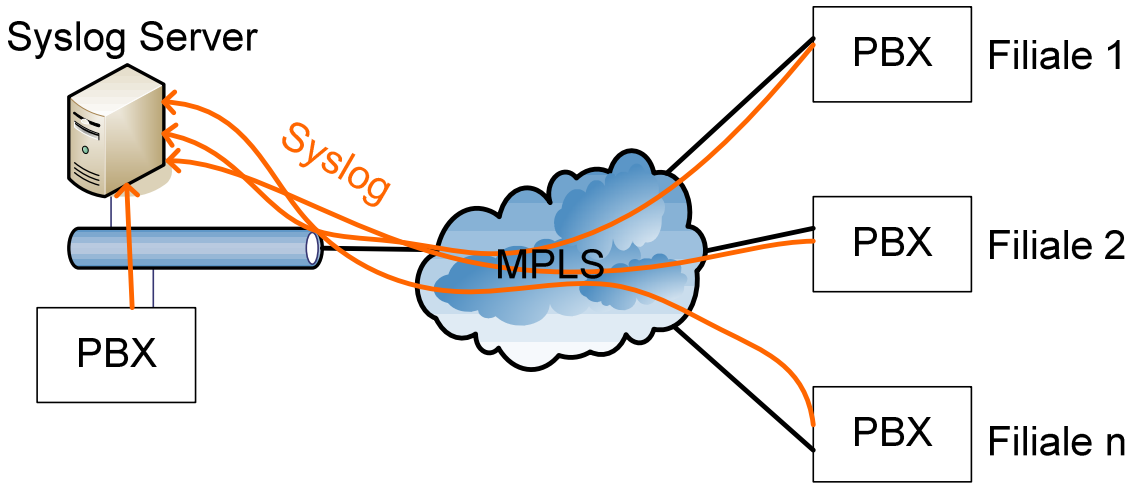


Abbildung 3-4: Syslog-Server mit mehreren PBXen

Betreffende Syslog-Meldungen werden nur bei einem Gesprächsaufbau und -abbau sowie bei anderen Signalisierungsvorgängen, wie einer Vermittlung, an den Server gesendet und enthalten neben den RTCP-basierenden Qualitätswerten auch andere Merkmale des Gesprächs.

3.2 Installation des Monitoring-Systems

Eine von vielen Möglichkeiten einen Syslog-Server zu realisieren, ist die Serversoftware Splunk. Diese Variante bietet nicht nur die Möglichkeit Syslog als Datenquelle zu definieren, sondern es können auch viele andere Quellen definiert werden. Für die Auswertung der RTCP-Daten ist zunächst nur die Verwendung von Syslog interessant.

Um einen Mehrwert der Installation zu erreichen bzw. die Installation so kosteneffizient wie möglich zu gestalten, kann die Lösung virtualisiert und auf derselben virtuellen Maschine eine Lösung für das Netzwerkmanagement installiert werden. Für diesen Zweck eignet sich die Managementlösung Nagios, die gut in eine Gesamtlösung mit Splunk integriert werden kann. Weiters ist, zusätzlich zum frei verfügbaren Modul Nagios, eine Möglichkeit für grafische Konfiguration zu empfehlen, die hier noch nicht integriert ist. Zu diesem Zweck wurde die Lösung Nconf gewählt, wobei es auch dazu einige Alternativen gibt.

Zur Analyse der Syslog-Meldungen wird nur das Modul Splunk verwendet. Der Vollständigkeit halber wird auch die Installation der Bestandteile Nagios und NConf behandelt.

Wenn von einer virtualisierten Serverumgebung ausgegangen wird, zeigt sich die Architektur des Servers wie in **Abbildung 3-5**.

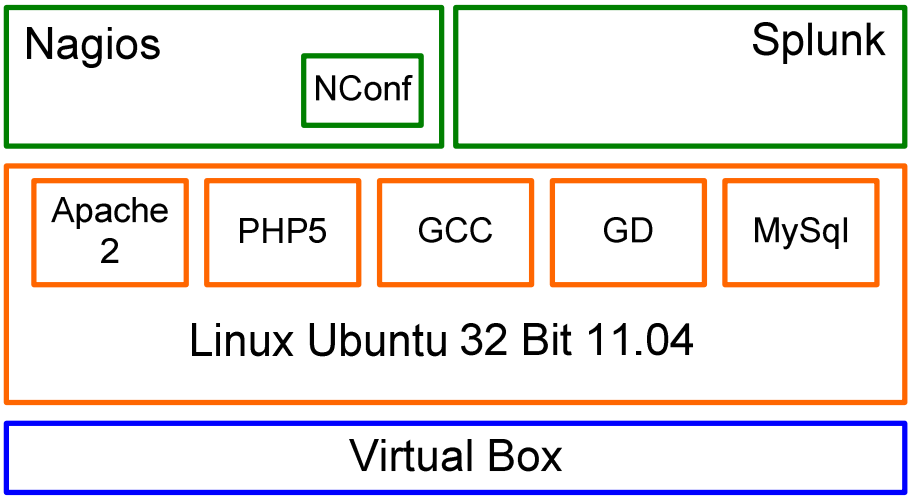


Abbildung 3-5: Mögliche Architektur des Servers beim Einsatz von Nagios + Splunk

Als Basis dient die 32-Bit-Version der Linux-Distribution Ubuntu 11.04, die in eine virtuelle Umgebung mit Oracle Virtual Box integriert ist. Die virtuelle Umgebung kann durch die eines alternativen Herstellers, zum Beispiel VMWare, beliebig ersetzt werden. Als weitere

Softwarepakete, welche gleichzeitig die Grundlage für die Installation von Nagios und Splunk bilden, müssen der Webserver Apache 2, PHP5, der aktuelle GCC (Gnu Compiler Collection) mit Bibliotheken und GD-Bibliotheken (Gif Draw) installiert werden. Für die Archivierung der Syslog-Daten werden mindestens 2 GB freier Speicherplatz benötigt, um die Software Splunk lauffähig zu halten.

3.2.1 Vorbereitung des Betriebssystems

Als Betriebssystem werden von Nagios ausschließlich Linux-Distributionen unterstützt, Splunk wäre aber auch auf Windows-Plattformen lauffähig. Als gemeinsamer Nenner kommen damit mehrere Linux-Distributionen in Frage, wobei Ubuntu aufgrund der weiten Verbreitung und der Vorteile, die damit verbunden sind, eine gute Wahl ist. Die IP-Adresse des Servers wird, wie bei Servern üblich, statisch konfiguriert. Weiters muss genug freier Speicherplatz, mindestens 2 GB, für die Anforderung auf dem Server vorhanden sein.

Die entsprechenden Erweiterungen für das Betriebssystem können im Linux-Shell mit der Funktion apt-get installiert werden. Mit diesem Befehl wird die aktuelle Version der Komponenten automatisch von den Paketquellen der Linux-Distribution geladen. Demnach lassen sie sich bei vorhandener Internetverbindung mit folgenden Befehlen installieren:

- sudo apt-get install apache2
- sudo apt-get install libapache2-mod-php5
- sudo apt-get install build-essential
- sudo apt-get install libgd2-xpm-dev
- sudo apt-get install mysql

Die Befehle wurden mit Ubuntu 11.04 getestet, möglicherweise weichen die nötigen Befehle bei anderen Versionen des Betriebssystems ab. Eine manuelle Installation der Softwarepakete ist ebenfalls möglich.

Weiters ist es zu empfehlen, auf dem Server eine Möglichkeit zur Remotewartung herzustellen. Eine Möglichkeit hierfür ist VNC (Virtual Network Computing).

3.2.2 Installation der Softwarepakete von Nagios, NConf und Splunk

Jedes dieser Softwaremodule steht in der aktuellen Version als *.tar.gz-Datei auf der Homepage des Herstellers bzw. des Entwicklerteams zur Verfügung.

Die Bestandteile und Quellen der aktuellen Versionen lauten wie folgt:

- **Nagios:**
  Dieser quelloffene Bestandteil der Implementierung stellt den Kern der Überwachungslösung (Monitoringlösung) zur Verfügung.

http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.3.tar.gz

- **NConf:**
  NConf ist eine Erweiterung für Nagios, welche die Konfiguration über eine grafische Oberfläche mit einem Webbrowser ermöglicht. Diese Softwareerweiterung benötigt eine MySQL-Datenbank.

  http://sourceforge.net/projects/nconf/files/nconf/1.2.6-0/nconf-1.2.6-0.tgz/download

- **Splunk:**
  Jenes Modul, das Möglichkeiten zur Auswertung von Syslog-Meldungen ermöglicht, ist Splunk.

  http://www.splunk.com/index.php/download_track?file=4.2.1/splunk/linux/splunk-4.2.1-98164-Linux-i686.tgz&platform=Linux&architecture=x86&version=4.2.1&typed=release&name=linux_installer&d=pro

Grundsätzlich werden die Dateien vor der Installation mit folgenden Befehlen extrahiert:

tar xzvf nagios-3.2.3.tar.gz

tar xzvf splunk-4.2.1-98164-Linux-i686.tgz

Die Zahlenfolge im Dateinamen ist dabei durch die gegebene Version zu ersetzen.

Die Dateien für NConf müssen in das Verzeichnis /var/www extrahiert werden:

tar xzvf nconf-1.2.6.tar.gz

Anschließend ist das mitgelieferte Installationsskript im Installationsverzeichnis von Nagios auszuführen. Zum Beispiel:

./configure --with-command-group=nagcmd

Für detaillierte Beschreibungen der Installation sind die dazugehörigen Dokumente /Nagios2011/, /NConf2011/ und /Splunk2011/ hinzuzuziehen.

3.2.3 Konfiguration von Nagios mittels NConf

Wenn die Nagios-Lösung mit der NConf-Erweiterung richtig auf dem Server installiert wurde, kann die weitere Konfiguration über die NConf-Oberfläche über den Webbrowser erfolgen:

http://172.25.96.201/Install.php

Anschließend wird der Benutzer durch einen Installationsprozess geführt, der die Softwarevoraussetzungen überprüft und die Anbindung an die MySQL-Datenbank

einrichtet. Srceenshots inkl. Kommentaren für durchzuführende Einstellungen zur Einrichtung von NConf sind in **Anlagen, Teil1** zu finden. Nachdem das Setup ausgeführt wurde, müssen die Dateien INSTALL, INSTALL.php, UPDATE und UPDATE.php im Verzeichnis /var/www/ gelöscht werden.

Weitere Hinweise für die Konfiguration und die Bedienung der Oberfläche sind im NConf Quickstart Guide und in dazugehöriger Dokumentation verfügbar. /NconfQs2011/

Wurde die Konfiguration durchgeführt, muss sie vom NConf-Installationsordner in den Konfigurationsordner von Nagios kopiert und Nagios neu gestartet werden:

tar -xf /var/www/output/NagiosConfig.tgz -C /usr/local/nagios/etc/objects/

/etc/init.d/nagios restart

Weitere Methoden zur Aktivierung der Konfiguration sind zu finden unter /NConfCd2011/.

3.2.4 Konfiguration von Splunk

Nachdem die Installation von Splunk erfolgreich abgeschlossen wurde, kann die Konfiguration des Moduls vorgenommen werden. Auf die Konfiguration von Nagios wird hier nicht weiter eingegangen, da sie in dieser Anwendung jene von Splunk nicht beeinflusst.

Der Zugriff auf die Konfigurationsoberfläche geschieht über den Webbrowser mit Port 8000:

http://172.25.96.201:8000

Nach der Anmeldung können verschiedene Datenquellen für Logdaten definiert werden. Hier ist für Syslog eine UDP-Quelle auf Port 514 zu definieren.

Weiters sind alle Endgeräte und PBXen, die an der Analyse der Gesprächsqualität teilnehmen sollen, so zu konfigurieren, dass sie Syslog-Meldungen an den Splunk-Server schicken.

Wenn alle Einstellungen vorgenommen sind, werden alle Datenquellen am Server zentral aufgezeichnet. Detaillierte Beschreibungen der einzelnen Konfigurationsschritte sind in /Splunk2011/ zu finden.

3.2.5 Konfiguration der PBX

Bei einer Innovaphone-PBX ist, wie in **Abbildung 3-6** dargestellt wird, der Splunk-Server im Menüpunkt *Gateway/CDR0* oder *Gateway/CDR1* als Empfänger für Syslog einzutragen.

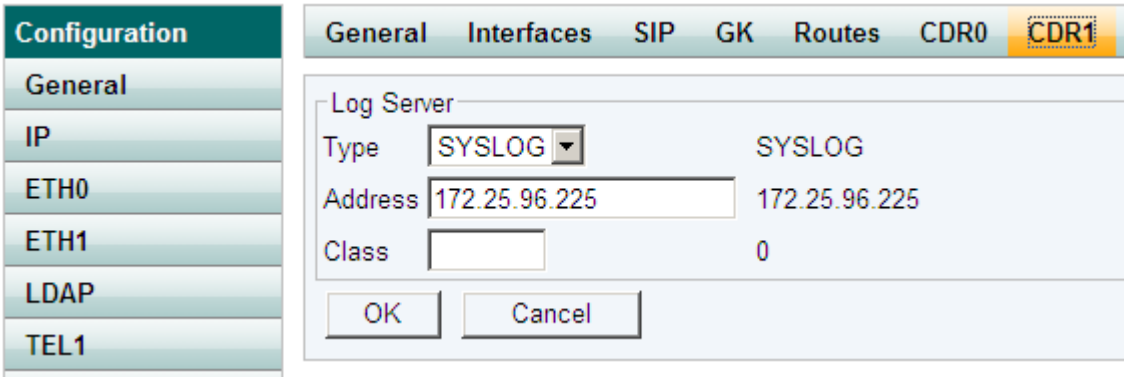


Abbildung 3-6:Konfiguration einer Innovaphone-PBX für Syslog

Diese Konfiguration kann in einem Verbund mit mehreren Filialen bzw. bei der Verwendung von mehreren PBXen an jedem Standort gleich vorgenommen werden.

4 Auswertung der Ergebnisse

In diesem Abschnitt werden die Ergebnisse der Auswertung der Syslog-Daten am Server erläutert und einige Vor- und Nachteile dieser Lösung aufgezeigt. Weiters werden einige Empfehlungen zur Implementierung und Verbesserungsvorschläge gegeben.

4.1 Auswertung der Syslog-Daten am Server

Die Oberfläche von Splunk kann mit einem Webbrowser aufgerufen werden:

http://172.25.96.225:8000

Nach erfolgreichem Login erscheint bei einem funktionsfähigen Server die in **Abbildung 4-1** dargestellte Oberfläche.

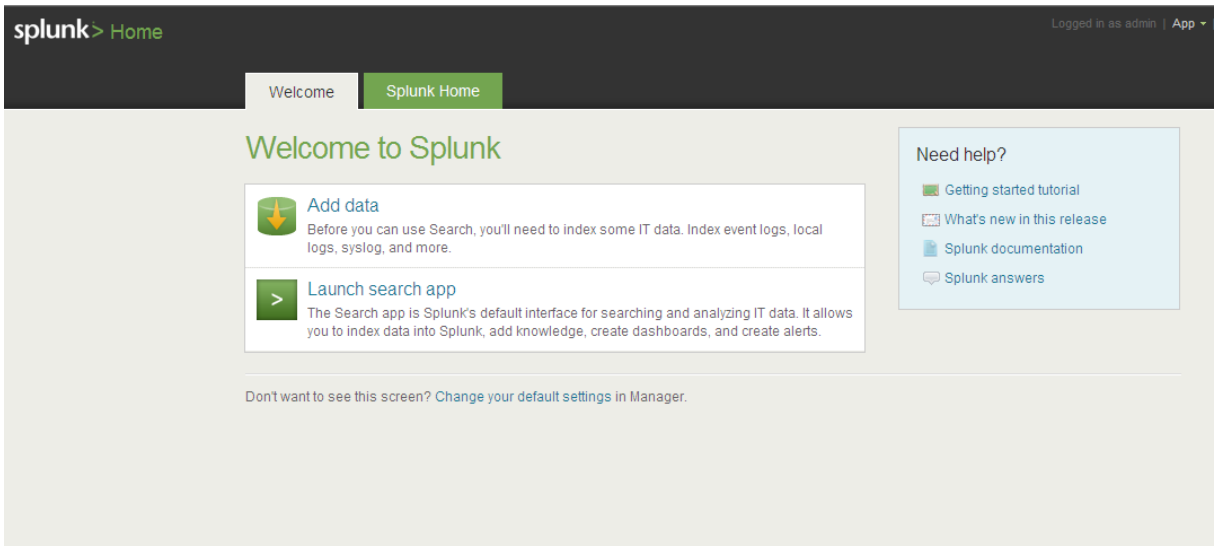


Abbildung 4-1: Startbildschirm von Splunk

Mit Launch search app können anschließend auf dem Server alle bisher eingegangenen Syslog-Meldungen angezeigt werden. **Abbildung 4-2** zeigt einen Überblick über die Syslog-Meldungen verschiedener Quellen. Wie hier ersichtlich ist, sind auf diesem Server von verschiedenen Quellen 422 Syslog-Meldungen auf den Ziel-UDP-Port 514 eingegangen. Diese Meldungen stammen von vier verschiedenen Innovaphone-PBXen, was man an den vier verschiedenen IP-Adressen erkennen kann.

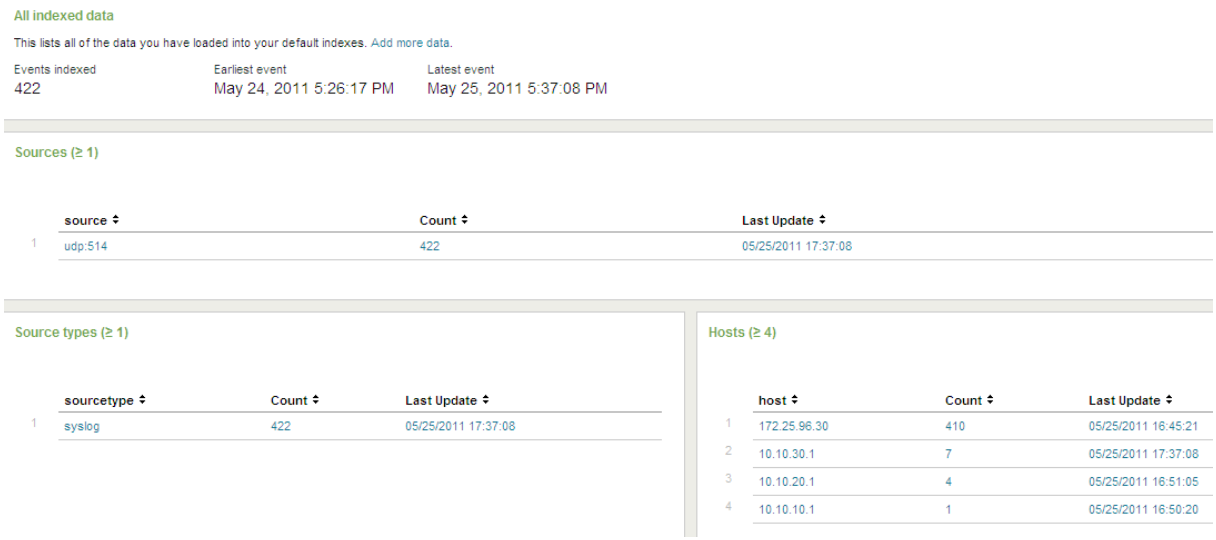


Abbildung 4-2: Suchüberblick der Syslog-Meldungen in Splunk

Für die weitere Analyse werden die Einträge der PBX *172.25.96.30* betrachtet. Die dazugehörigen Syslog-Meldungen können per Mausklick auf die IP-Adresse aufgerufen werden.

4.2 Syslog-Meldungen von Testgesprächen

Wenn die Einstellungen wie in **Abschnitt 3.2.5** vorgenommen wurden, erzeugt jedes Gespräch mehrere Syslog-Meldungen, die an den Server gesendet werden. Dabei werden bei einem einfachen Gespräch jeweils bei Gesprächsaufbau, dem Gespräch selbst und bei Gesprächsabbau eigene Einträge erzeugt. Die Anzahl der generierten Syslog-Meldungen pro Gespräch ist davon abhängig, ob während des Verlaufs weiterverbunden, eine Konferenzschaltung aktiviert wurde oder andere Funktionen der PBX genutzt wurden.

Abbildung 4-3 zeigt einige Basisszenarien, deren Qualität mittels Syslog-Meldungen im folgenden Abschnitt analysiert wird: Kommunikation in einem LAN, über MPLS und über WLAN mit einem WLAN-fähigen Endgerät.

Alle Meldungen beinhalten Werte für RTT, Jitter und Paketverlust. Die vollständige Ausgabe an Meldungen ist in **Anlagen, Teil 2** aufgeführt.

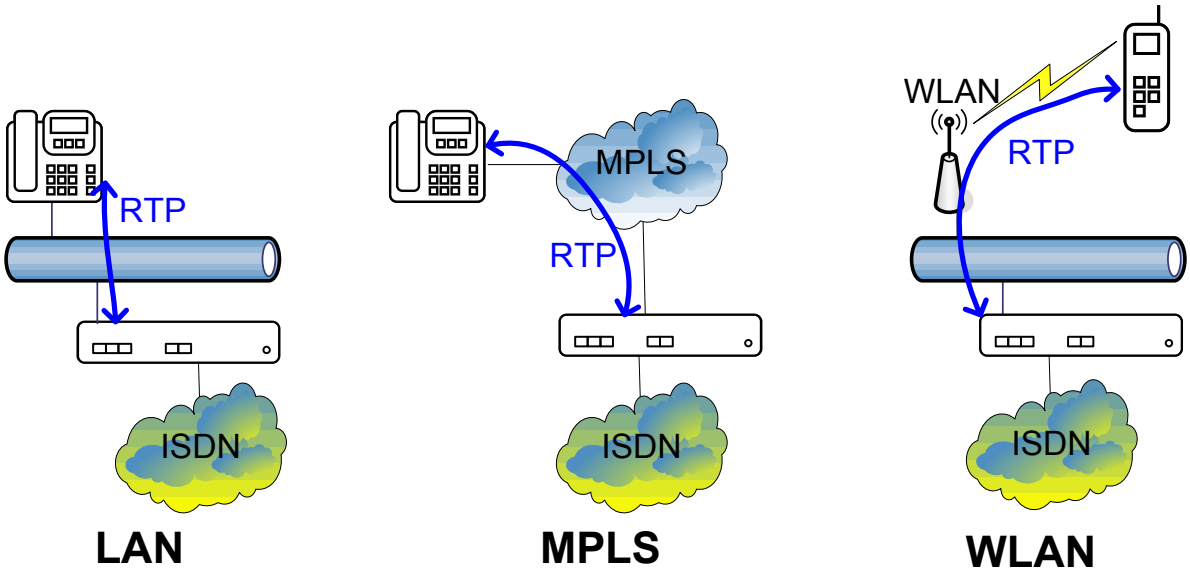


Abbildung 4-3: Untersuchte Testszenarien

4.2.1 Gespräch in einem LAN

Bei einem Gespräch in einem LAN wurden die hier aufgeführten Einträge erzeugt. Als Endgerät wurde der Typ Innovaphone IP200A verwendet, als PBX und Gateway der Typ IP302. Der Strom der RTP-Pakete verläuft dabei zwischen den Geräten direkt über ein LAN, basierend auf Ethernet mit 100 Mbit/s.

Während des Gesprächs werden mehrere Meldungen generiert, die in **Anlagen, Teil 2** aufgeführt sind. Die höchste Aussagekraft hat die Meldung, die am Ende des Gesprächs generiert wird, weil hier die Summe aller verlorenen Pakete ersichtlich ist sowie die genauesten Durchschnittswerte für Jitter und RTT.

5/31/11 8:39:51.000 PM	*May 31 20:39:51 172.25.96.30 ?event=B:Rel&time=1306867192&date=20110531-183952&ref=fcbef555e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(1,0,0)&rcoder=G711A,30(1,0,0)&xstats=1+1+0+0+0&rstats=1+2+0+0+0&alert_time=1306867117&connect_time=1306867118&disc_time=1306867187&srv_id=00-90-33-1e-05-32*

Tabelle 4-1: Syslog-Meldung bei einem Gespräch im LAN

Wie aus der Meldung ersichtlich ist, gibt es mehrere Felder, die ausgewertet werden können. Von Interesse sind insbesondere die Felder *xstats* und *rstats*.

xstats beschreibt die Qualität des von der PBX gesendeten RTP-Stroms. Voraussetzung für die Richtigkeit dieser Werte ist eine korrekte und kompatible Implementierung von RTCP am Endgerät bzw. der Gegenstelle.

xstats=1+1+0+0+0

Die fünf Felder bezeichnen die durchschnittliche RTT, die maximale RTT, den durchschnittlichen Jitter, den maximalen Jitter und den Paketverlust.

Die Qualität des RTP-Stroms, der von der PBX empfangen wird, wird vom Feld *rstats* beschrieben. /InnoWiki2011/

rstats=1+2+0+0+0

Die Bedeutung der Felder entspricht jener von *xstats*.

In diesem Fall sind die Übertragungsbedingungen ideal, da alle Werte für Jitter und Packet Loss null sind. Gemessene Werte von wenigen Millisekunden (hier: 1-2 ms) für RTT sind ebenfalls als ideal anzusehen.

4.2.2 Gespräch über MPLS

Anders stellt sich ein Syslog-Eintrag eines Gesprächs, das über eine MPLS-Leitung mit einer verfügbaren Bandbreite von 2 Mbit/s von Innsbruck nach Wien geführt wird, dar. Vom Endgerät (IP200A) aus verläuft der RTP-Strom dabei über die MPLS-Leitung zur PBX (IP6000). **Tabelle 4-2** zeigt den letzten Eintrag dieses Gesprächs. Der MPLS-Anschluss wird zu diesem Zeitpunkt nicht durch andere Datenübertragungen belastet.

6/3/11 6:22:36.000 PM	*Jun 3 18:22:36 172.25.29.30 ?event=B:Rel&time=1307118155&date=20110603-162235&ref=d2c1cc03e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(20,0,0)&rcoder=G711A,60(20,0,0)&xstats=20+20+0+0+0&rstats=20+20+0+0+0&alert_time=1307118138&connect_time=1307118141&disc_time=1307118153&srv_id=00-90-33-08-02-d5&charge_units=1*

Tabelle 4-2: Syslog-Meldung bei einem Gespräch über MPLS

Die Werte für *xstats* und *rstats* lauten:

xstats=20+20+0+0+0

rstats=20+20+0+0+0

Wie hier zu erkennen ist, sind während des Gesprächs keine Pakete verloren gegangen und der Wert für Jitter ist null. RTT ist auf dieser Übertragungsstrecke jedoch auf 20 gestiegen. Da die Werte für maximale und durchschnittliche RTT gleich sind, kann weiters angenommen werden, dass die Übertragungsbedingungen während des Gespräches weitgehend gleich geblieben sind.

Wenn auf der Übertragungsstrecke keine Priorisierung für VoIP eingerichtet ist, ist zu erwarten dass sich die Messwerte verschlechtern, insbesondere dann, wenn die Strecke durch andere Datenübertragung ausgelastet ist. **Tabelle 4-3** zeigt den letzten Syslog-

Eintrag eines Gesprächs, wenn parallel dazu ein Datentransfer die MPLS-Leitung belastet.

6/6/11 5:13:55.000 PM	*Jun 6 17:13:55 172.25.29.30 ?event=B:Rel&time=1307373235&date=20110606-151355&ref=94fda748e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(42,11,1)&rcoder=G711A,60(56,0,0)&xstats=42+58+8+11+1&rstats=56+58+0+0+0&alert_time=1307373187&connect_time=1307373188&disc_time=1307373233&srv_id=00-90-33-08-02-d5&charge_units=2*

Tabelle 4-3: Syslog-Meldung bei einem Gespräch über MPLS unter Last

Die Werte für *xstats* und *rstats* lauten hier:

xstats=42+58+8+11+1

rstats=56+58+0+0+0

Diese Werte sind bereits deutlich schlechter als jene, die bei der unbelasteten Leitung gemessen wurden. Folglich wirkt sich eine ausgelastete Leitung ohne QoS-Merkmale negativ auf die Gesprächsqualität aus.

Insgesamt ist die Qualität bei der Verwendung von MPLS für die Übertragung über WANs sehr gut im Vergleich zu anderen Methoden, die hier zur Verfügung stehen.

4.2.3 Gespräch über WLAN

Weitaus ungünstiger stellen sich die Werte dar, wenn das Gespräch über WLAN geführt wird. Die Qualität hängt hier stark von realisierten QoS-Merkmalen, Interferenzen, Signalstärke und anderen Kriterien ab. Als Endgerät dient in diesem Fall ein Smartphone (Samsung Galaxy S) mit SIP-Clientsoftware eines anderen Herstellers (Sipdroid).

6/3/11 6:31:34.000 PM	*Jun 3 18:31:34 172.25.96.30 ?event=B:Disc&time=1307118694&date=20110603-163134&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,7,21)&xstats=0+0+0+0+0&rstats=0+0+4+7+21&alert_time=1307118630&connect_time=1307118633&disc_time=1307118694&srv_id=00-90-33-1e-05-32*

Tabelle 4-3: Syslog-Meldung bei einem Gespräch über WLAN

Die Werte für *xstats* und *rstats* lauten:

xstats=0+0+0+0+0

rstats=0+0+4+7+21

Bei diesem Beispiel fallen mehrere nicht ideale Eigenschaften des Rufs auf:

- Alle Werte im Feld *xstats* sind nicht korrekt bzw. nicht realistisch. Daraus ist zu schließen, dass die RTCP-Implementierung im Endgerät (Sipdroid) nicht vorhanden oder nicht kompatibel ist.
- Es sind gar keine Werte für RTT vorhanden, da für die Berechnung eine richtige Implementierung in der PBX und im Endgerät nötig ist.
- Dennoch ist hier ersichtlich, dass die Übertragung über WLAN einen durchschnittlichen Jitter-Wert von 4 ms erzeugt. Der maximale Wert liegt bei 7 ms, weshalb anzunehmen ist, dass der Wert einer Schwankung unterliegt.
- Während der Dauer des Gesprächs sind 21 Pakete verloren gegangen. Die Dauer liegt bei einer Minute, was aus der zeitlichen Differenz des Gesprächs zwischen erstem und letztem dazugehörigen Syslog-Eintrag oder den Gesprächsdaten aus dem letzten Syslog-Eintrag ersichtlich ist.

4.3 Qualitätsanalyse mit Splunk

Die Softwarelösung bietet eine Vielzahl an Funktionen, um Syslog-Meldungen zu bearbeiten. Eine Auswahl davon, die hier behandelt wird, ist insbesondere für VoIP von Interesse.

4.3.1 Ermittlung des prozentuellen Paketverlusts

Eine Syslog-Meldung beinhaltet keine Werte für den prozentuellen Paketverlust. Die Felder *connect_time* und *disc_time* erlauben die Ermittlung der Gesprächsdauer t. Die Anzahl der theoretisch insgesamt übertragenen Pakete ergibt sich in Abhängigkeit von der Paketzeit (ptime = 30 ms). Das Verhältnis der verlorenen Pakete zu den in Summe übertragenen ergibt den prozentuellen Paketverlust.

connect_time=1307118633

disc_time=1307118694

$$t := disc\_time - connect\_time$$

$$P_{gesamt} := \frac{t}{ptime}$$

$$PL_{Prozentuell} := \frac{P_{verloren}}{P_{gesamt}} \cdot 100\%$$

Die Berechnung ergibt angewandt auf die Messergebnisse der Syslog-Meldungen von **Abschnitt 4.2.3** einen Paketverlust von 1%.

4.3.2 Erweiterte Suchabfragen und Statistiken

Für die Analyse von Qualität in VoIP sind in den Syslog-Meldungen einige Werte besonders aussagekräftig. Die Möglichkeiten der Suchabfragen sollen hier anhand einiger Beispiele dargestellt werden. Detaillierte Dokumentationen zu den einzelnen Funktionen sind unter /Splunk2011/ nachzulesen.

Beispiel 1: Filter auf Codec

Es sollen Einträge der PBX 172.25.96.30 angezeigt werden, die mit dem Codec G.711A geführt wurden. Hierzu kann einfach eine neue Suchabfrage mit folgendem Befehl generiert werden:

host="172.25.96.30" g711a

Diese Abfrage untersucht alle Meldungen auf dem Server und gibt nur Syslog-Meldungen aus, die den Kriterien entsprechen. Das Ergebnis sind somit alle Aufzeichnungen über Gespräche, die mit dem Codec G.711a geführt wurden.

Beispiel 2: Filter auf RTT, Jitter oder Packet Loss

Splunk bietet die Möglichkeit, nach beliebigen Feldern zu filtern. Ein Feld ist dadurch gekennzeichnet, dass dem Feldinhalt eine Feldbezeichnung gefolgt von „=“ vorangeht. Beispielsweise ergibt folgender Ausdruck als Ausgabe alle Einträge, die Qualitätswerte tragen:

*rstats=**

Weiters liefert die grafische Oberfläche die Möglichkeit, Statistiken für einen bestimmten Zeitraum zu generieren. Hier wurde das Feld *rstats* gewählt und alle Gespräche wurden dargestellt. Durch die Auswertung werden alle Werte für RTT, Jitter und Paketverlust ersichtlich, außerdem werden die Anzahl der Meldungen und deren prozentueller Anteil dargestellt.

Value	#	%
0+0+0+0+0	746	86.443%
1+1+0+0+0	54	6.257%
19+19+0+0+0	8	0.927%
2+2+0+0+0	7	0.811%
1+1+0+0+2	5	0.579%
1+1+0+0+3	5	0.579%
63+63+0+0+0	4	0.463%
1+2+0+0+33	3	0.348%
1+2+0+0+53	3	0.348%
1+2+0+0+10	3	0.348%

Abbildung 4-4: Statistik verschiedener Qualitätswerte

Die Ansicht ermöglicht einen guten Überblick über die Gespräche im Netzwerk. Wie hier ersichtlich ist, stehen die meisten Einträge für gute Qualität.

Dieser Eintrag belegt mindestens ein Gespräch bei dem RTT 63 ms beträgt:

63+63+0+0+0

Weitere Einträge weisen auf Gespräche hin, bei denen während der Übertragung einige Pakete verloren gegangen sind:

1+2+0+0+33

1+2+0+0+53

Die hier gezeigte Darstellung ist auch durch andere Möglichkeiten zu ergänzen.

In **Abbildung 4-5** ist die entsprechende Statistik mit zeitlichem Verlauf über zwei Tage als logarithmische Balkendarstellung abgebildet.

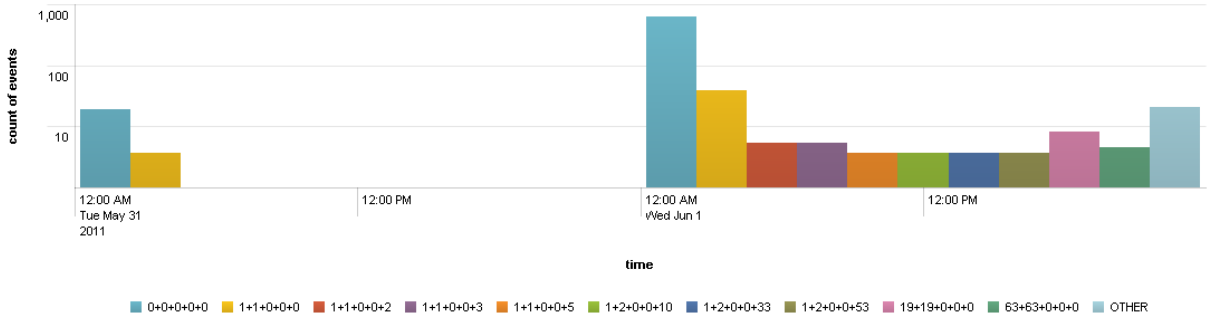


Abbildung 4-5: Auswertung mit zeitlichem Verlauf

Bei optionaler, genauerer Eingrenzung des Zeitraumes auf eine relevante Spanne ergibt sich eine Darstellung wie in **Abbildung 4-6** gezeigt.

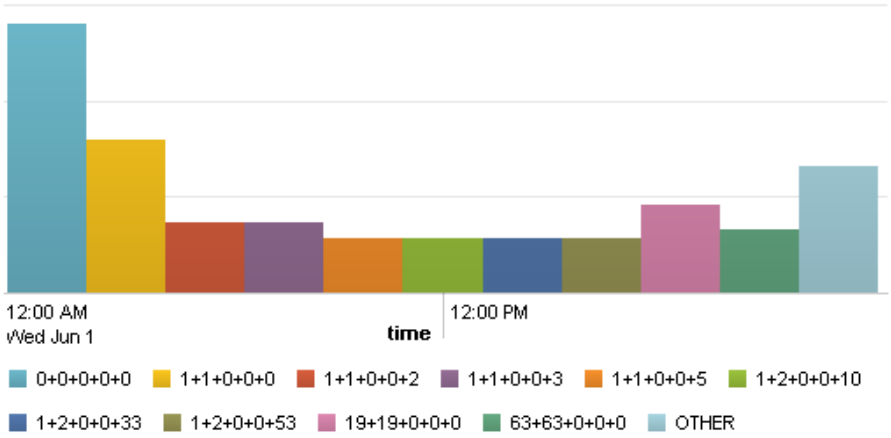


Abbildung 4-6: Auswertung eines Auszugs des zeitlichen Verlaufs

Aus diesen Ansichten wird auch ersichtlich, wie sich die Anzahl und die Qualität der Gespräche im Zeitverlauf verändern. In diesem Beispiel wurden am Dienstag, dem 31. Mai, wenige Gespräche, bei denen nur gute Qualitätswerte zu sehen sind, geführt. Für den 1. Juni sind wesentlich mehr Einträge zu sehen, unter denen auch jene zu finden sind, die auf schlechte Gesprächsqualität hinweisen.

Splunk bietet noch viele weitere Möglichkeiten zur statistischen Auswertung entsprechender Syslog-Meldungen. Die angewandten Methoden richten sich nach den Erfordernissen in einem Unternehmen. /Splunk2011/

4.3.3 Alarmbenachrichtigungen

In Kombination mit Suchabfragen ist es möglich, eine Aktion im Alarmfall auszulösen. Bei dieser Anwendung ist es sinnvoll, bei der Überschreitung eines bestimmten Wertes für RTT, Jitter oder Paketverlust eine Benachrichtigung per E-Mail zu verschicken. Die Konfiguration der Alarmbenachrichtigung erfolgt dabei in drei Schritten, die in **Abbildung 4-7** dargestellt werden:

- **Definition der Suchabfrage (Save Search):**
  Zuerst muss eine Abfrage definiert werden, deren Ergebnis den Alarm auslöst. Beispielweise trifft der Suchausdruck *Xstats>20* zu, wenn die durchschnittliche RTT größer als 20 ms ist.

- **Definition der Bedingung für einen Alarm (Set up Alert):**
  Aufgrund verschiedener Merkmale des Suchergebnisses kann ein Alarm generiert werden. In diesem Fall soll eine Meldung gesendet werden, wenn die Suchabfrage mindestens ein Ergebnis liefert.

- **Definition der Alarmaktion (Define Actions):**
  Bei dieser Anwendung ist die Alarmierung per E-Mail am sinnvollsten. Eine andere Aktion wäre beispielsweise das Ausführen eines Skripts am Server.

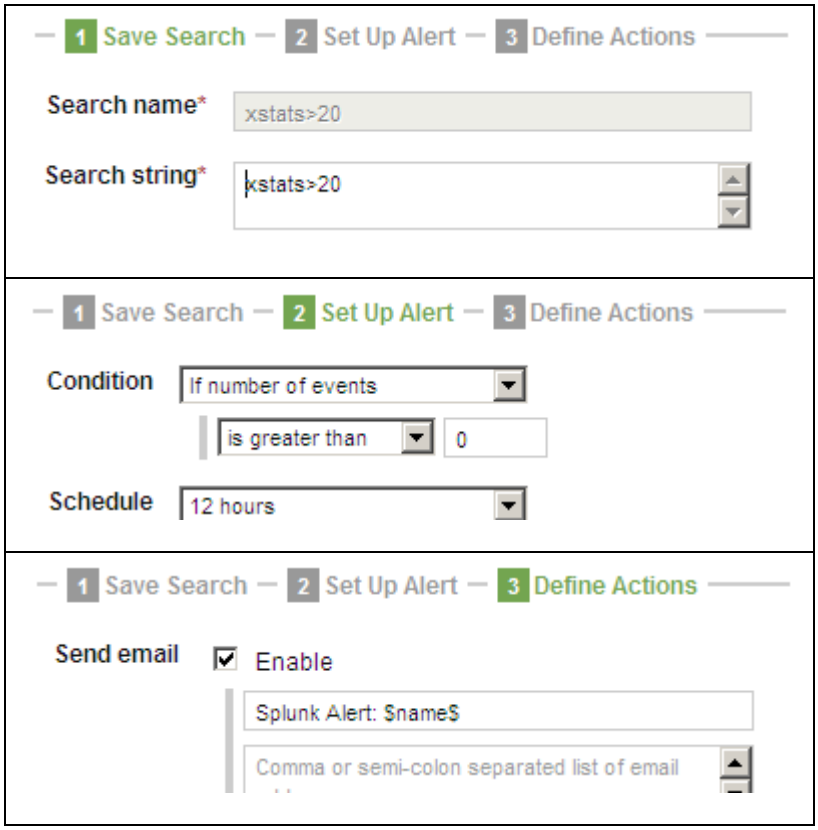


Abbildung 4-7: Konfigurationsschritte für eine Alarmbenachrichtigung

4.4 Anwendung der Überwachungslösung in einem Unternehmen

Die hier dargestellten Möglichkeiten zur Auswertung reichen allein nicht aus, um Qualitätsprobleme von VoIP erfolgreich zu bearbeiten. Die Verfahren müssen auch richtig angewandt werden, um auf verschiedene Fehlerszenarien mit den passenden Mitteln reagieren zu können. Deshalb sollte der Anwender der Monitoringlösung, in der Regel der Systemadministrator, über einen passenden Leitfaden verfügen, nach dem man sich beim Auftreten eines Problems richten kann. Ein Vorschlag für die Anwendung in einem Unternehmen beliebiger Größe ist in **Abbildung 4-8** dargestellt. Die hier gezeigte Variante ist ein Grundgerüst, das, je nach Anforderungen des Unternehmens, verfeinert und erweitert werden kann. Der Anstoß für die Verwendung von Splunk ist dabei idealerweise eine Alarmmeldung, die vom Administrator per E-Mail oder auf ähnlichem Weg empfangen wurde. Auch Mängel, die von einem Benutzer gemeldet werden, können der Grund für eine Analyse mit Splunk sein. Durch die Anbindung von Geräten aus der Netzwerkinfrastruktur an die Gesamtlösung kann im besten Fall die Fehlerursache sofort gefunden werden; in anderen Fällen muss die Umgebung des Gesprächs genauer untersucht werden, um zu einer Lösung zu kommen. Beispielsweise ist es aufgrund von

Syslog-Meldungen nicht unmittelbar ersichtlich, ob ein organisatorisches Problem, wie in **Kapitel 2.1** beschrieben, vorliegt.

Hinweise auf Qualitätsprobleme:

Hinweise auf Probleme mit der VoIP-Qualität sind Alarmmeldungen von Splunk oder Beschwerden eines Benutzers. Bei einer kundengerechten Konfiguration von Splunk tritt die Alarmmeldung auf, bevor es zu einer Beschwerde des Benutzers kommt.

Bestätigung des Problems:

Unter Zuhilfenahme der Suchfunktionen in Splunk werden entsprechende Syslog-Einträge gesucht und dem als fehlerhaft gemeldeten Ruf zugeordnet.

Suche nach weiteren Hinweisen auf das Problem:

Es wird nach weiteren Fehlermeldungen gesucht, die zum selben Zeitpunkt wie der mangelhafte Ruf aufgetreten sind und mit dem Problem in Verbindung gebracht werden können.

Behebung des Problems:

Wenn im zeitlichen Umfeld des Fehlers auf dem Server auch Meldungen anderer Geräte (z.B. aus der Netzwerkinfrastruktur) aufgetreten sind, die einen Hinweis auf ein Problem enthalten, sollten die betreffenden Geräte als nächstes untersucht werden.

Falls keine derartigen Hinweise am Server zu finden sind, sollten alle Geräte, die als Ursache in Frage kommen, aber nicht in die Überwachung eingebunden sind, untersucht werden.

Dazu gehört auch das Endgerät, insbesondere dessen analoge Komponenten wie Kabel, Hörerschnüre, Headsets etc.

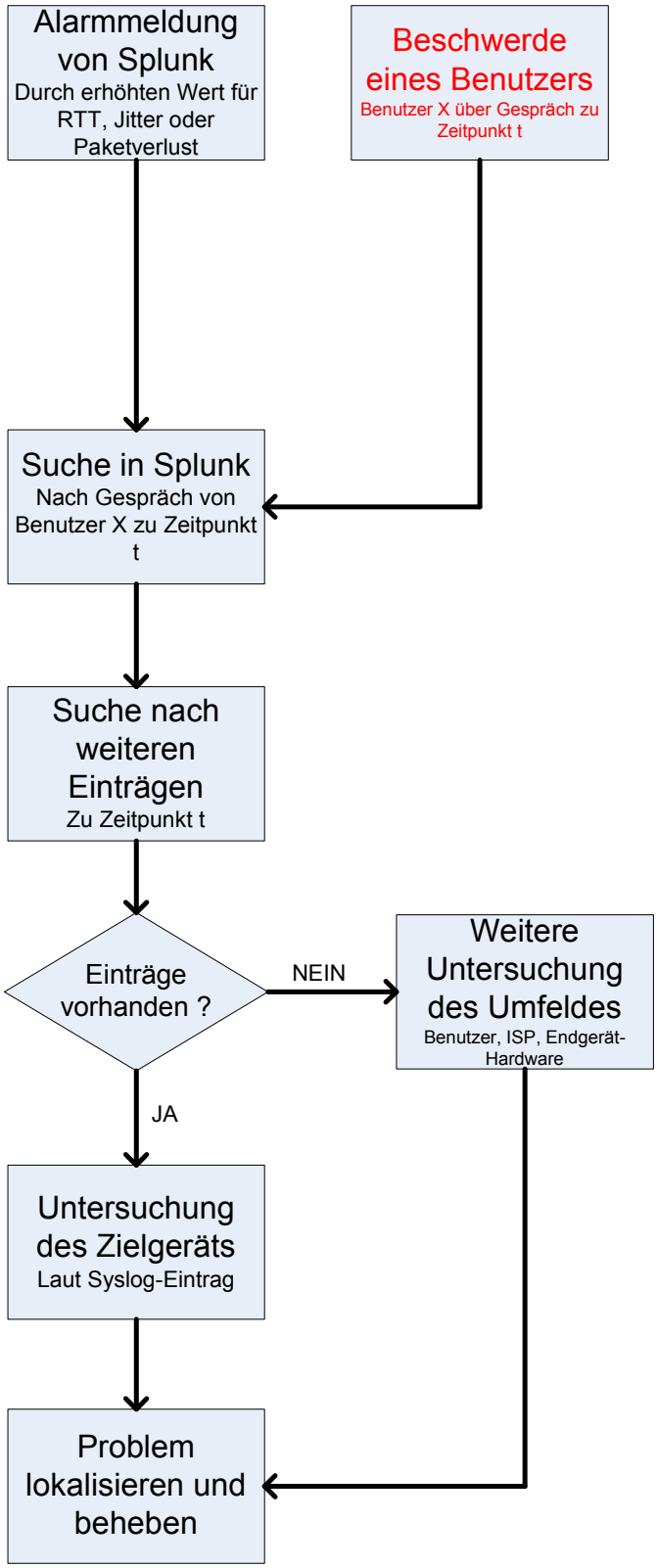


Abbildung 4-8: Ablauf beim Auftreten eines Fehlerfalls

4.5 Verbesserungsmöglichkeiten

Die Möglichkeit, RTCP-Kennwerte mithilfe von Syslog und Splunk auszuwerten, bietet einem Systemadministrator einen passenden Zugang, um Qualitätsprobleme bei VoIP zu analysieren. Die Softwarelösung bietet einige gute Varianten, die Syslog-Meldungen zu speichern und nach bestimmten Mustern zu suchen. Weiters sind viele Mittel implementiert, um die Werte anschaulich darzustellen.

Es gibt dennoch einige Wege, um diese Lösung zu verbessern.

4.5.1 Häufigkeit von RTCP-Meldungen

Die RTCP-Werte liegen unabhängig von der Länge des Gesprächs nur am Anfang und am Ende des Gesprächs vor. Zur Darstellung von Qualitätsänderungen während eines Gesprächs müssten die Daten häufiger und regelmäßig übertragen werden.

In einer PBX werden die Werte alle 10 s aktualisiert. Es könnte eine Möglichkeit implementiert werden, um Werte mit derselben Frequenz an den Syslog-Server zu senden.

Die momentane Implementierung in der PBX sieht vor, dass im Wesentlichen nur die Kennwerte am Ende des Gesprächs aussagekräftige Werte für die Analyse liefern.

Eine regelmäßige Übertragung der Daten bedarf allerdings einer Softwaremodifikation des Herstellers.

4.5.2 Kompatibilität der Endgeräte

Wie am Beispiel in **Abschnitt 4.2.3** gezeigt wurde, sind die Umsetzungen von RTCP bei Fremdherstellern oft unzureichend. Um die Zuverlässigkeit der gelieferten Werte zu gewährleisten, muss kontrolliert werden, ob deren Implementierungen zu jener in der PBX kompatibel sind.

Endgeräte, deren Verhalten in Bezug auf RTCP nicht genau bekannt ist, müssen getestet werden, bevor sie in die Überwachung durch Splunk eingebunden werden. Eine mangelnde Implementierung von RTCP hat zur Folge, dass die Werte in der Syslog-Meldung immer *rstats=0+0+0+0+0* oder *xstats=0+0+0+0+0* lauten, was als ideale Übertragung interpretiert wird, selbst wenn es in Wirklichkeit keine ideale Übertragung ist.

Es sollte deshalb darauf geachtet werden, dass solche Endgeräte aus dem Überwachungsprozess ausgeschlossen werden, sofern auf deren Einsatz verzichtet werden kann.

4.5.3 Einbinden anderer Geräte der Infrastruktur

Da Splunk auch zu jedem anderen, syslogfähigen Gerät kompatibel ist, kann man sich dessen Funktion auch für andere Anwendungen zu Nutze machen. Beispielsweise lassen sich beliebige Geräte der Netzwerkinfrastruktur einbinden. **Abbildung 4-9** zeigt ein

fiktives Beispiel in Anlehnung an die bereits behandelten Bestandteile eines typischen Netzes bei der Anwendung von VoIP. Bei vielen dieser Komponenten ist es nützlich, den Splunk-Server als Empfänger für Syslog-Meldungen zu definieren. Zunächst ist es von Vorteil, beliebige Server, auch jene, die keine Dienste für VoIP bereitstellen sowie den Splunk-Server selbst, mit einzubinden.

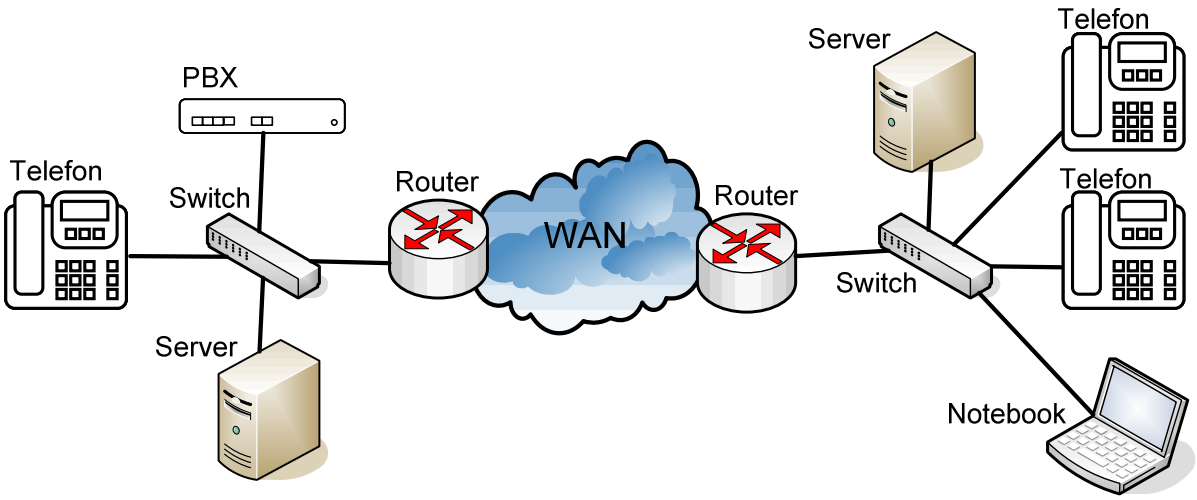


Abbildung 4-9: Syslogfähige Geräte im Netzwerk

Viele Komponenten der Netzwerkinfrastruktur, Router oder Switches, sind ebenfalls zu Syslog kompatibel. Deren Anbindung erlaubt es, bei der Fehleranalyse einen detaillierteren Blick auf ein eventuell vorhandenes Problem zu bekommen.

Da Probleme mit VoIP häufig von Fehlern in der Netzwerkinfrastruktur abhängig sind, ist die Einbindung dazugehöriger Komponenten in das System überaus sinnvoll. Das erlaubt eine weitere Analyse einer Problemstellung auf derselben Plattform. Eine Syslog-Meldung von einem Router oder Switch zu einem Zeitpunkt, zu dem Qualitätsprobleme im Netzwerk aufgetreten sind, kann einen entscheidenden Hinweis bei der Suche nach der Ursache geben.

5 Zusammenfassung

5.1 Ergebnisse

Diese Diplomarbeit hatte es zum Ziel, die notwendigen Mittel zur Untersuchung von Qualitätsproblemen zu untersuchen und eine geeignete Methode umzusetzen.

Um an solche Problemstellungen richtig herantreten zu können, ist es notwendig, sich mit den Grundlagen von VoIP auseinanderzusetzen, speziell mit jenen Aspekten, die für das Qualitätsempfinden durch den Benutzer relevant sind. Diese Punkte wurden im einleitenden theoretischen Teil behandelt.

Weiters war es wichtig, alle möglichen Einflüsse der Übertragung von Sprache über IP zu untersuchen. Als Grundlage hierfür dienten einfache Testaufbauten von Rufverläufen, um die Aussagekraft einzelner Kennwerte abzuwägen und zu untersuchen. Hierfür wurde dieses Thema in mehrere Teilgebiete abgegrenzt.

Es wurden für die Untersuchung der organisatorischen Einflüsse auf VoIP die Methoden der Paketbildung genauer betrachtet, insbesondere deren Auswirkung auf die tatsächlich benötigte Bandbreite von Gesprächen über VoIP. Außerdem wurden die notwendigen Kennwerte für RTT, Jitter und Paketverlust auf deren Aussagekraft untersucht, und abschließend die Einflüsse betrachtet, die das Endgerät auf die Übertragung nimmt. Es wird festgestellt, dass die Implementierungen in den Endgeräten und im Netzwerk zwar maßgeblichen Einfluss auf die Gesprächsqualität haben, die größte Beeinträchtigung können aber organisatorische Defizite, wie eine nicht ideale Wahl der Übertragungsstrecken oder der Sprachcodierung, zur Folge haben.

Als Ergebnis dieser Untersuchungen wurde eine passende Lösung gewählt, um die anfangs definierten Anforderungen umsetzen und die Kennwerte passend darstellen zu können. Die Wahl fiel dabei auf die serverbasierende Lösung Splunk, die in einer virtuellen Umgebung und basierend auf Linux umgesetzt wurde. Weiters wurde auf demselben Server eine auf Nagios und NConf basierende allgemeine Netzwerk-Monitoringlösung integriert, um zu demonstrieren, dass mehr Nutzen aus der Gesamtlösung gezogen werden kann.

Anschließend wurde die firmeninterne Telefonieumgebung in dieses System eingebunden. Die Anbindung selbst erwies sich in diesem Fall als einfach, da das Protokoll Syslog als Schnittstelle zwischen den Telefonanlagen und dem Server verwendet wurde. Außerdem trug die bereits vorhandene und fehlerfreie Implementierung wesentlich dazu bei.

Bei der Untersuchung der Auswertungsmöglichkeiten anhand von typischen Rufverläufen im LAN, über MPLS oder WLAN wurde deutlich, dass es starke Qualtätsunterschiede

zwischen den Übertragungsmöglichkeiten gibt, was sich auch richtig in den RTCP-Protokolldaten zeigt. Beispielsweise ist die Gesprächsqualität über MPLS oder WLAN schlechter als im LAN, wobei mit MPLS gute Werte bei der Übertragung über ein WAN zu erreichen sind.

Für die Betrachtung der Ergebnisse, die mit Splunk erzielt werden konnten, war die Anwendung von Nagios und NConf nicht mehr notwendig. Die Serversoftware wurde auf Möglichkeiten untersucht, um die Messwerte in Statistiken und Graphen auszuwerten. Einige Beispiele für diese Möglichkeiten, die Splunk zur Darstellung der Werte liefert, wurden hier aufgezeigt. Diese Lösung beinhaltet jedoch noch eine Vielzahl an anderen Möglichkeiten, auf die nicht weiter eingegangen werden konnte. Die Implementierung von Splunk hängt im Endeffekt von verschiedenen Anforderungen des Netzwerks ab, beispielsweise von der Größe, von der Architektur sowie von der Menge und dem Typ der Endgeräte.

5.2 Ausblick

Die vorliegende Herangehensweise an Problemstellungen im Bereich der Qualität von VoIP behandelt zwar viele Gesichtspunkte, wobei sich die Wichtigkeit der einzelnen Kennwerte aber im Laufe der Zeit verändern wird. Dies rührt von den eingesetzten Basistechnologien her, wie MPLS, IP oder Ethernet, da sie einer steten Weiterentwicklung unterliegen. Es ist anzunehmen, dass zum Beispiel Ethernet in den nächsten Jahren durch weitere Technologien ergänzt wird und diese eine Verbesserung der Übertragungsqualität bieten werden. Die laufende Weiterentwicklung dieser Basistechnologien hat es unter anderem zum Ziel, die Übertragungsqualität in Bezug auf Verzögerungen, Jitter und Paketverlust zu verbessern, was auch VoIP zugute kommt. Es ist zu erwarten, dass die hier angestellten Überlegungen in Zukunft zwar auch zutreffen, aber durch verschiedene Weiterentwicklungen an Wichtigkeit verlieren werden, weil die Netze ein besseres Maß an Qualität bereitstellen oder bereits vorhandene Möglichkeiten eine breitere Anwendung finden werden. Auch die hier dargestellten Berechnungen für den Bandbreitenbedarf eines Gesprächs dürften mit den Jahren aufgrund des weiteren Anstiegs der verfügbaren Bandbreite durch die Provider nicht mehr in diesem Ausmaß relevant sein. Ebenso ist abzusehen, dass die hier verwendeten Sprachcodecs G.711 und G.729 zunehmend durch modernere Verfahren abgelöst werden. Insbesondere G.711 dürfte mit der Verdrängung von ISDN aus der Telefonie in lokalen Netzen durch Wideband-Codecs ersetzt werden.

Für jede professionelle Umsetzung von VoIP wird es aber immer notwendig sein, ein Bewusstein für Qualität und einflussnehmende Faktoren in einem Unternehmen zu entwickeln und zu behalten. Durch den andauernden Siegeszug von VoIP wird das in Zukunft noch wichtiger sein als heute, auch wenn sich die verwendeten Technologien verändern werden.

Die Implementierung mit Splunk kann nach den hier dargestellten Möglichkeiten weiter verbessert werden. In diese Lösung kann außerdem jedes Gerät, das über passende

Schnittstellen und Protokolle zur Anbindung verfügt, in das Netz eingebunden werden. Die dargestellte Kombination von Nagios und Splunk ist heute eine weit verbreitete und akzeptierte Lösung. Der Nutzen in Bezug auf die Qualitätsüberwachung bei VoIP hängt dabei hauptsächlich davon ab, welche Möglichkeiten die Telefonanlage bietet. Mit Innovaphone, dem hier verwendeten Hersteller, lassen sich über Syslog gute Ergebnisse erzielen, auch wenn manche Stellen noch verbessert werden können. Theoretisch lassen sich ähnliche Ergebnisse mit nahezu jedem beliebigen Hersteller erreichen.

Literatur

/Badach2007/ Anatol Badach: Voice over IP – Die Technik: Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit, 3. Auflage, Verlag Hanser, München 2007, ISBN 3-446-40666-2

/Fischer2008/ Jörg Fischer: VoIP – Praxisleitfaden, Verlag Hanser, München 2008, ISBN 978-3-446-41188-3

/Freyer2002/ Ulrich Freyer: Nachrichten-Übertragungstechnik, 5. Auflage, Verlag Hanser, München 2002, ISBN 3-446-22087-9

/BadHoff2007/ Badach, Hoffmann: Technik der IP-Netze, Funktionsweise, Protokolle und Dienste, 2. Auflage, Verlag Hanser, München 2007, ISBN 978-3-446-21935-9

/Lipp2006/ Manfred Lipp: VPN –Virtuelle Private Netzwerke, Verlag Addison-Wesley, München 2006, ISBN 978-3-8273-2252-4

/Sauter2011/ Martin Sauter: Grundkurs Mobile Kommunikationssysteme, 4. Auflage, Verlag Vieweg & Teubner, Berlin 2011, ISBN 978-3-8348-1407-4

/FreyBoss2008/ Frey, Bossert: Signal- und Systemtheorie, 2. Auflage, Verlag Vieweg & Teubner, Berlin 2008, ISBN 978-3-8351-0249-1

/Wiki2011/ Wikipedia: Allgemeine Informationen zu VoIP, http://www.wikipedia.org, verfügbar am 20.05.2011

/ITU2011/ ITU-T: Standards, http://www.itu.int/ITU-T/, verfügbar am 20.05.2011

/IETF2011/ IETF: Standards, http://www.ietf.org, verfügbar am 20.05.2011

/Xiph2011/ Xiph.org: Open Protocols and Software, http://xiph.org, verfügbar am 21.05.2011

/NConf2011/ NConf: Installation Guide, http://www.nconf.org/dokuwiki/doku.php?id=nconf:help:documentation:installation#manual_installation_commandline, verfügbar am 28.05.2011

/Nagios2011/ Nagios: Quickstart Guide-Ubuntu, http://nagios.sourceforge.net/docs/3_0/quickstart-ubuntu.html, verfügbar am 28.05.2011

/Splunk2011/ Splunk: Dokumentation, http://www.splunk.com/base/Documentation, verfügbar am 28.05.2011

/NconfQs2011/ NConf: Quickstart Guide, http://www.nconf.org/dokuwiki/doku.php?id=nconf:help:documentation:quick-start_guide, verfügbar am 29.05.2011

/NconfCd2011/ NConf: Configuration Deployment, http://www.nconf.org/dokuwiki/doku.php?id=nconf:help:documentation:howtos:configuration_deployment, verfügbar am 29.05.2011

/InnoWiki2011/ Innovaphone: Wikiseite, http://wiki.innovaphone.com, verfügbar am 15.05.2011

/Shark2011/ Wireshark: Netzwerksniffer, http://www.wireshark.org, verfügbar am 12.05.2011

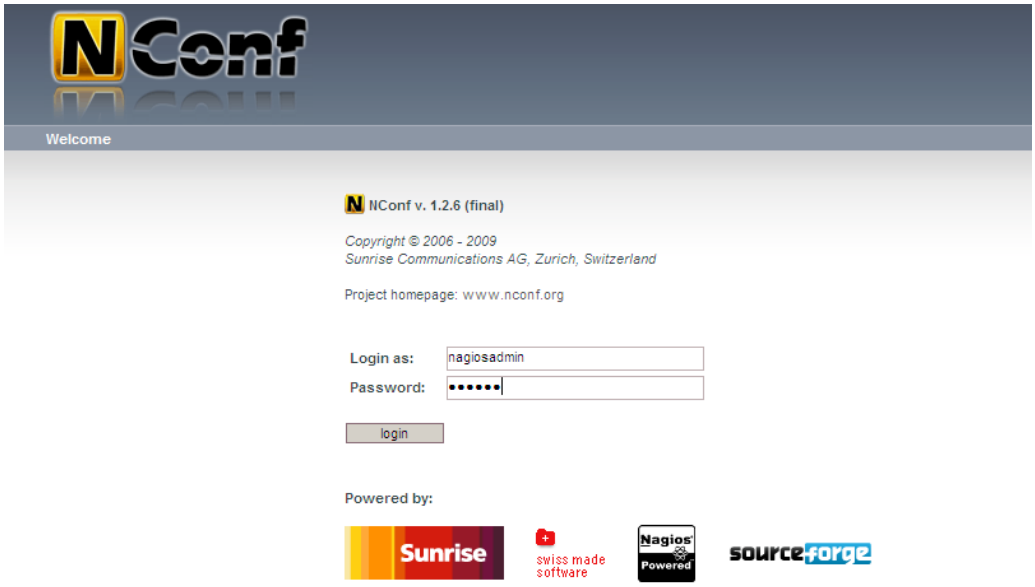
/Innovaphone2011/ Innovaphone: Homepage, http://www.innovaphone.com, verfügbar am 15.05.2011

Anlagen

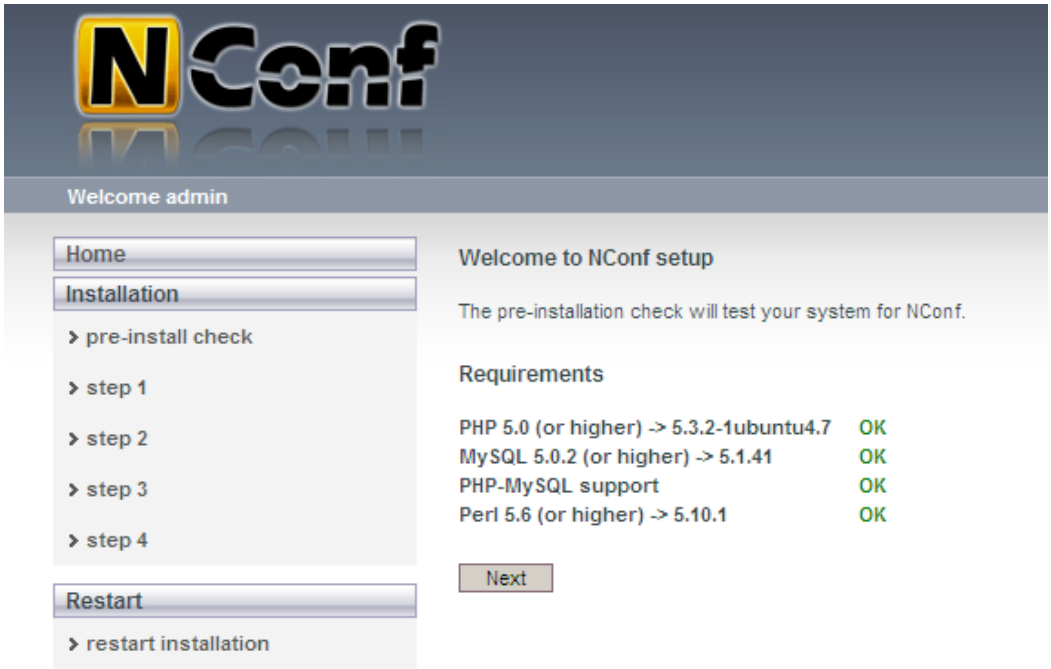
Anlagen, Teil 1

Im folgenden Abschnitt wird die Konfiguration von NConf in einer Schritt-für Schritt-Anleitung beschrieben.

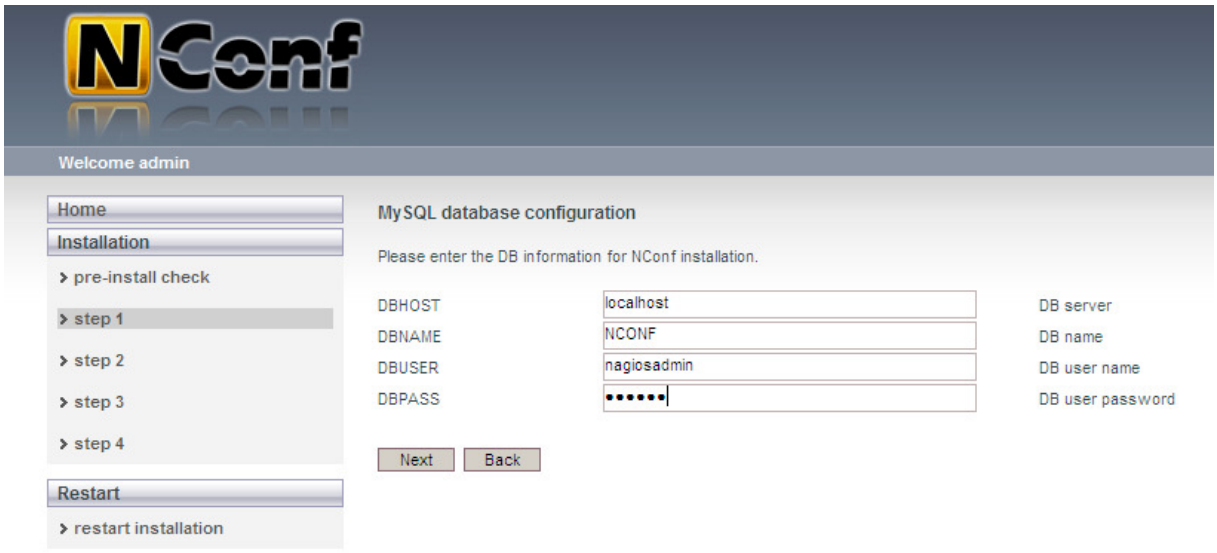
1) Login:



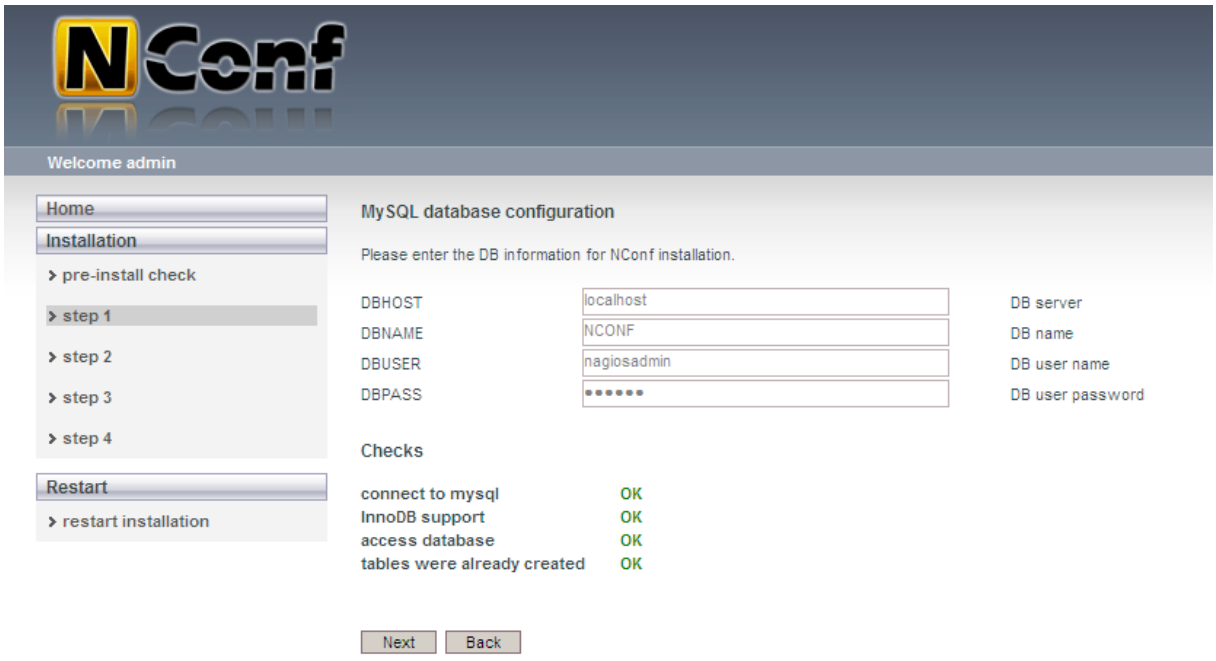
2) Überprüfung der Systemvoraussetzungen: Alle hier aufgelisteten Pakete müssen vorhanden sein und zum Fortfahren auf „OK“ stehen.



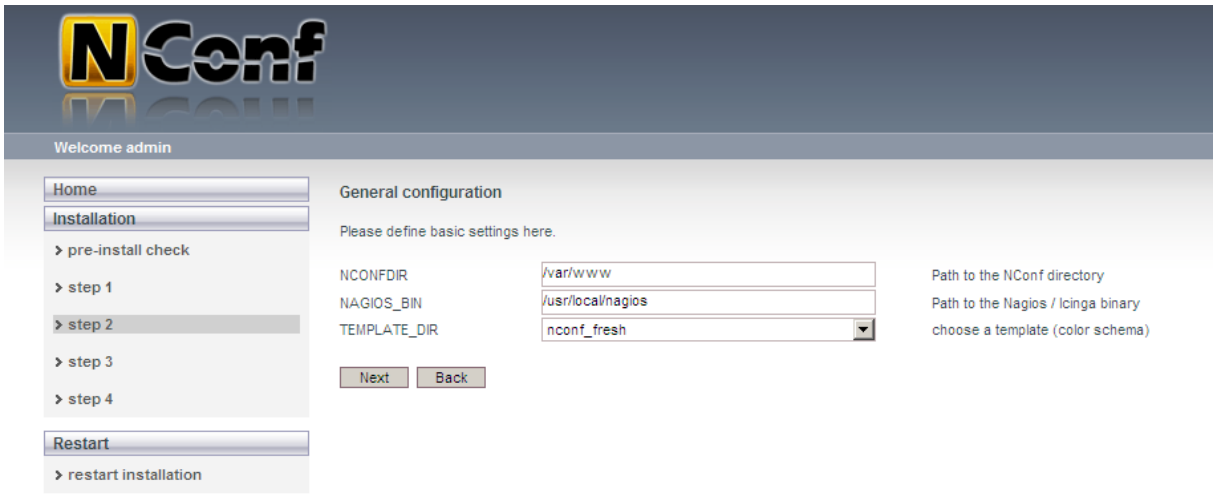
3) Anlegen einer Datenbank in MySQL:



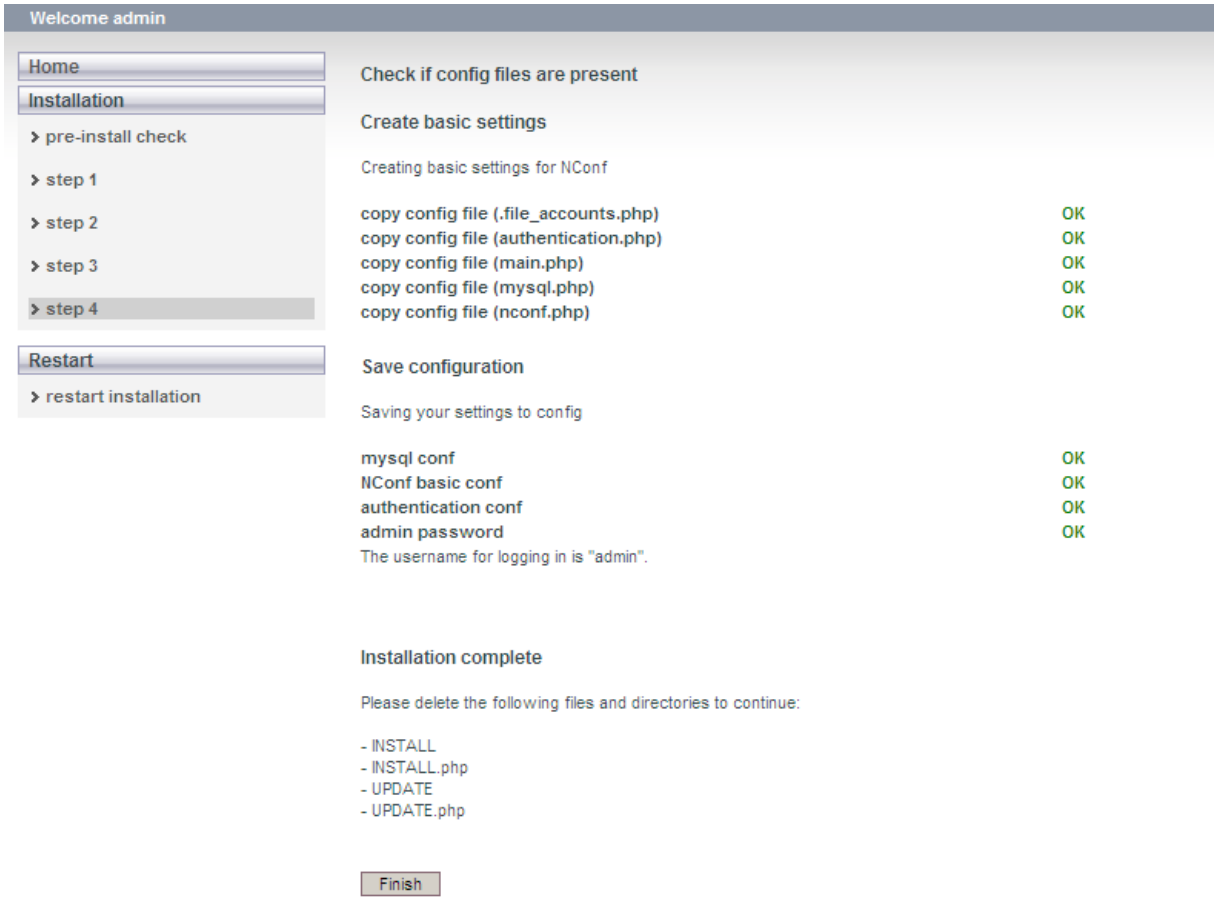
4) Nach dem erfolgreichen Anlegen der MySQL-Datenbank müssen alle Meldungen auf „OK“ stehen.



5) Kontrolle der Installationspfade:



6) Wenn die Konfiguration richtig vorgenommen wurde, werden alle Einträge mit „OK“ gekennzeichnet.



Anlagen, Teil 2

Im Folgenden sind alle Syslog-Meldungen der getätigten Testgespräche aufgelistet.

1) Gespräch in einem LAN:

06.06.2011 *5:45:52.000 PM*	*Jun 6 17:45:52 172.25.96.30 ?event=B:Rel&time=1307375154&date=20110606-154554&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(1,0,0)&xstats=0+0+0+0+0&rstats=1+1+0+0+0&alert_time=1307375142&connect_time=1307375146&disc_time=1307375150&srv_id=00-90-33-1e-05-32*
06.06.2011 *5:45:52.000 PM*	*Jun 6 17:45:52 172.25.96.30 <cdr guid="93bade57e909d311b1e200903308002a" sys="PBX001" pbx="ATINN1" node="ATINN1" device="ATINN1 Trunk" cn="ATINN1 Trunk" e164="006648149308" dir="to" utc="1307375137" local="1307382337"><event msg="setup-to" time="0" e164="6012" h323="Schwanninger F." conf="1f0a450ee909d311a3ee009033102ba9"/><event msg="alert-from" time="5" e164="6012" h323="Schwanninger F."/><event msg="conn-from" time="9" e164="6012" h323="Schwanninger F."/><event msg="disc-from" time="13" cause="16"/><event msg="rel-to" time="16" cause="16"/></cdr>*
06.06.2011 *5:45:52.000 PM*	*Jun 6 17:45:52 172.25.96.30 ?event=A:Rel&time=1307375154&date=20110606-154554&ref=1f0a450ee909d311a3ee009033102ba9&dir=in&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(1,0,0)&xstats=0+0+0+0+0&rstats=1+1+0+0+0&alert_time=1307375142&connect_time=1307375146&disc_time=1307375150&srv_id=00-90-33-1e-05-32*
06.06.2011 *5:45:52.000 PM*	*Jun 6 17:45:52 172.25.96.30 <cdr guid="ea13430ee909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP200A-10-2b-a9" cn="Schwanninger F." e164="6012" h323="Schwanninger F." dir="from" utc="1307375137" local="1307382337"><event msg="setup-from" time="0" e164="006648149308" conf="1f0a450ee909d311a3ee009033102ba9"/><event msg="alert-to" time="5" e164="*06006648149308"/><event msg="conn-to" time="9" type="ext" e164="006648149308"/><event msg="disc-to" time="13" cause="16"/><event msg="rel-from" time="16" cause="16"/></cdr>*
06.06.2011 *5:45:49.000 PM*	*Jun 6 17:45:49 172.25.96.30 ?event=B:Disc&time=1307375150&date=20110606-154550&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(1,0,0)&xstats=0+0+0+0+0&rstats=1+1+0+0+0&alert_time=1307375142&connect_time=1307375146&disc_time=1307375150&srv_id=00-90-33-1e-05-32*
06.06.2011 *5:45:45.000 PM*	*Jun 6 17:45:45 172.25.96.30 ?event=B:Connect&time=1307375146&date=20110606-154546&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url*

	=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307375142&connect_time=1307375146&srv_id=00-90-33-1e-05-32
06.06.2011 5:45:41.000 PM	*Jun 6 17:45:41 172.25.96.30 ?event=B:Alert&time=1307375142&date=20110606-154542&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307375142&srv_id=00-90-33-1e-05-32*
06.06.2011 5:45:36.000 PM	*Jun 6 17:45:36 172.25.96.30 ?event=B:Proceed&time=1307375137&date=20110606-154537&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.06.2011 5:45:36.000 PM	*Jun 6 17:45:36 172.25.96.30 ?event=Media&time=1307375137&date=20110606-154537&ref=1f0a450ee909d311a3ee009033102ba9&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.06.2011 5:45:36.000 PM	*Jun 6 17:45:36 172.25.96.30 ?event=B:Call&time=1307375137&date=20110606-154537&ref=1f0a450ee909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.06. 20115:45:36.000 PM	*Jun 6 17:45:36 172.25.96.30 ?event=A:Call&time=1307375137&date=20110606-154537&ref=1f0a450ee909d311a3ee009033102ba9&dir=in&src_if=GW1&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*

2) Gespräch über MPLS ohne Belastung der Verbindung:

06.03.2011 6:22:36.000 PM	*Jun 3 18:22:36 172.25.29.30 ?event=B:Rel&time=1307118155&date=20110603-162235&ref=d2c1cc03e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(20,0,0)&rcoder=G711A,60(20,0,0)&xstats=20+20+0+0+0&rstats=20+20+0+0+0&alert_time=1307118138&connect_time=1307118141&disc_time=1307118153&srv_id=00-90-33-08-02-d5&charge_units=1*
06.03.2011 6:22:36.000 PM	*Jun 3 18:22:36 172.25.29.30 ?event=A:Rel&time=1307118155&date=20110603-162235&ref=d2c1cc03e909d311a3ee009033102ba9&dir=in&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(20,0,0)&rcod*

	er=G711A,60(20,0,0)&xstats=20+20+0+0+0&rstats=20+20+0+0+0&alert_time=1307118138&connect_time=1307118141&disc_time=1307118153&srv_id=00-90-33-08-02-d5&charge_units=1
06.03.2011 *6:22:36.000 PM*	*Jun 3 18:22:36 172.25.96.30 <cdr guid="c377dacae909d311bdbc0090331e0532" sys="PBX001" pbx="ATINN1" node="root" cn="_MASTER_" e164="0" dir="to" utc="1307118133" local="1307125333"><event msg="setup-to" time="0" e164="6012" h323="Schwanninger F." conf="d2c1cc03e909d311a3ee009033102ba9"/><event msg="alert-from" time="7" e164="6012" h323="Schwanninger F."/><event msg="conn-from" time="9" e164="6012" h323="Schwanninger F."/><event msg="disc-from" time="22" cause="16"/><event msg="rel-to" time="23" cause="16"/></cdr>*
06.03.2011 *6:22:36.000 PM*	*Jun 3 18:22:36 172.25.96.30 <cdr guid="ea13430ee909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP200A-10-2b-a9" cn="Schwanninger F." e164="6012" h323="Schwanninger F." dir="from" utc="1307118133" local="1307125333"><event msg="setup-from" time="0" e164="*00006648149308" conf="d2c1cc03e909d311a3ee009033102ba9"/><event msg="alert-to" time="7" e164="*00006648149308"/><event msg="conn-to" time="9" type="ext" e164="0"/><event msg="disc-to" time="22" cause="16"/><event msg="rel-from" time="23" cause="16"/></cdr>*
06.03.2011 *6:21:21.000 PM*	*Jun 3 18:21:21 172.25.29.30 ?event=B:Rel&time=1307118080&date=20110603-162120&ref=58114a42e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(0,0,0)&rcoder=G711A,60(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118071&connect_time=1307118075&disc_time=1307118078&srv_id=00-90-33-08-02-d5&charge_units=1*
06.03.2011 *6:21:21.000 PM*	*Jun 3 18:21:21 172.25.29.30 ?event=A:Rel&time=1307118080&date=20110603-162120&ref=58114a42e909d311a3ee009033102ba9&dir=in&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(0,0,0)&rcoder=G711A,60(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118071&connect_time=1307118075&disc_time=1307118078&srv_id=00-90-33-08-02-d5&charge_units=1*
06.03.2011 *6:21:21.000 PM*	*Jun 3 18:21:21 172.25.96.30 <cdr guid="c377dacae909d311bdbc0090331e0532" sys="PBX001" pbx="ATINN1" node="root" cn="_MASTER_" e164="0" dir="to" utc="1307118066" local="1307125266"><event msg="setup-to" time="0" e164="6012" h323="Schwanninger F." conf="58114a42e909d311a3ee009033102ba9"/><event msg="alert-from" time="6" e164="6012" h323="Schwanninger F."/><event msg="conn-from" time="10" e164="6012" h323="Schwanninger F."/><event msg="disc-from" time="13" cause="16"/><event msg="rel-to" time="15" cause="16"/></cdr>*
06.03.2011 *6:21:21.000 PM*	*Jun 3 18:21:21 172.25.96.30 <cdr guid="ea13430ee909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP200A-10-2b-a9" cn="Schwanninger F." e164="6012" h323="Schwanninger F." dir="from" utc="1307118066" local="1307125266"><event msg="setup-from" time="0" e164="*00006648149308" conf="58114a42e909d311a3ee009033102ba9"/><event msg="alert-to" time="6" e164="*00006648149308"/><event msg="conn-to" time="10" type="ext" e164="0"/><event msg="disc-to" time="13" cause="16"/><event msg="rel-from" time="15" cause="16"/></cdr>*

3) Gespräch über MPLS bei Belastung der Verbindung:

06.06.2011 *5:13:55.000 PM*	*Jun 6 17:13:55 172.25.29.30 ?event=B:Rel&time=1307373235&date=20110606-151355&ref=94fda748e909d311a3ee009033102ba9&dir=out&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(42,11,1)&rcoder=G711A,60(56,0,0)&xstats=42+58+8+11+1&rstats=56+58+0+0+0&alert_time=1307373187&connect_time=1307373188&disc_time=1307373233&srv_id=00-90-33-08-02-d5&charge_units=2*
06.06.2011 *5:13:55.000 PM*	*Jun 6 17:13:55 172.25.29.30 ?event=A:Rel&time=1307373235&date=20110606-151355&ref=94fda748e909d311a3ee009033102ba9&dir=in&src_if=GW1&dst_if=PRI1&src_cgpn=6012&src_cdpn=06648149308&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=06648149308&src_reg_name=ATVIE1-DT+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,60(42,11,1)&rcoder=G711A,60(56,0,0)&xstats=42+58+8+11+1&rstats=56+58+0+0+0&alert_time=1307373187&connect_time=1307373188&disc_time=1307373233&srv_id=00-90-33-08-02-d5&charge_units=2*
06.06.2011 *5:13:55.000 PM*	*Jun 6 17:13:55 172.25.96.30 <cdr guid="c377dacae909d311bdbc0090331e0532" sys="PBX001" pbx="ATINN1" node="root" cn="_MASTER_" e164="0" dir="to" utc="1307373182" local="1307380382"><event msg="setup-to" time="0" e164="6012" h323="Schwanninger F." conf="94fda748e909d311a3ee009033102ba9"/><event msg="alert-from" time="6" e164="6012" h323="Schwanninger F."/><event msg="conn-from" time="7" e164="6012" h323="Schwanninger F."/><event msg="disc-from" time="52" cause="16"/><event msg="rel-to" time="54" cause="16"/></cdr>*
06.06.2011 *5:13:55.000 PM*	*Jun 6 17:13:55 172.25.96.30 <cdr guid="ea13430ee909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP200A-10-2b-a9" cn="Schwanninger F." e164="6012" h323="Schwanninger F." dir="from" utc="1307373182" local="1307380382"><event msg="setup-from" time="0" e164="*00006648149308" conf="94fda748e909d311a3ee009033102ba9"/><event msg="alert-to" time="6" e164="*00006648149308"/><event msg="conn-to" time="7" type="ext" e164="0"/><event msg="disc-to" time="52" cause="16"/><event msg="rel-from" time="54" cause="16"/></cdr>*
06.06.2011 *5:11:50.000 PM*	*Jun 6 17:11:50 172.25.96.30 <cdr guid="eea5214de909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP230-1b-02-7d" cn="Unterlechner Martin" e164="6010" h323="Unterlechner M." dir="to" utc="1307373084" local="1307380284"><event msg="setup-to" time="0" e164="2225" h323="Mayrhofer K." conf="d61956d1e909d3119ce6009033100c81"/><event msg="alert-from" time="0" e164="2225" h323="Mayrhofer K."/><event msg="rel-to" time="27" cause="0"/></cdr>*
06.06.2011 *5:11:50.000 PM*	*Jun 6 17:11:50 172.25.96.30 <cdr guid="c377dacae909d311bdbc0090331e0532" sys="PBX001" pbx="ATINN1" node="root" cn="_MASTER_" e164="2225" h323="Mayrhofer K." dir="from" utc="1307373084" local="1307380284"><event msg="setup-from" time="0" e164="6010" conf="d61956d1e909d3119ce6009033100c81"/><event msg="alert-to" time="0" e164="6010" h323="Unterlechner M."/><event msg="rel-from" time="27" cause="0"/></cdr>*

4) Gespräch über WLAN:

06.03.2011 *6:31:34.000 PM*	*Jun 3 18:31:34 172.25.96.30 ?event=B:Disc&time=1307118694&date=20110603-163134&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&cause=02_80_90&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,7,21)&xstats=0+0+0+0+0&rstats=0+0+4+7+21&alert_time=1307118630&connect_time=1307118633&disc_time=1307118694&srv_id=00-90-33-1e-05-32*
06.03.20116:31:33.000 PM	*Jun 3 18:31:33 172.25.96.30 <cdr guid="93bade57e909d311b1e200903308002a" sys="PBX001" pbx="ATINN1" node="ATINN1" device="ATINN1 Trunk" cn="ATINN1 Trunk" e164="005123452006012" dir="from" utc="1307118630" local="1307125830"><event msg="setup-from" time="0" e164="6014" conf="b52c3605e909d311bdbc0090331e0532"/><event msg="alert-to" time="0" e164="6014" h323="Reiner H."/><event msg="conn-to" time="3" e164="6014" h323="Reiner H."/><event msg="rel-to" time="64" cause="0"/></cdr>*
06.03.2011 *6:31:33.000 PM*	*Jun 3 18:31:33 172.25.96.30 ?event=B:Rel&time=1307118694&date=20110603-163134&ref=b52c3605e909d311bdbc0090331e0532&dir=out&src_if=BRI1&dst_if=GW1&src_cgpn=05123452006012&src_cdpn=6014&dst_cgpn=05123452006012&dst_cdpn=6014&dst_url=hre@datentechnik.com&bcaps=03_80_90_a3&xcoder=G711A,30(1,0,0)&rcoder=G711A,30(0,0,0)&xstats=1+1+0+0+0&rstats=0+0+0+0+0&alert_time=1307118630&connect_time=1307118633&disc_time=1307118694&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:31:33.000 PM*	*Jun 3 18:31:33 172.25.96.30 <cdr guid="b9568f7de909d311ad0b00903308002a" sys="PBX001" pbx="ATINN1" node="root" device="IP200A-10-0c-93" cn="Reiner H." e164="6014" h323="Reiner H." dir="to" utc="1307118630" local="1307125830"><event msg="setup-to" time="0" type="ext" e164="005123452006012" conf="b52c3605e909d311bdbc0090331e0532"/><event msg="alert-from" time="0" e164="005123452006012"/><event msg="conn-from" time="3" type="ext" e164="005123452006012"/><event msg="rel-from" time="64" cause="0"/></cdr>*
06.03.2011 *6:30:33.000 PM*	*Jun 3 18:30:33 172.25.96.30 ?event=B:Connect&time=1307118633&date=20110603-163033&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118630&connect_time=1307118633&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:32.000 PM*	*Jun 3 18:30:32 172.25.96.30 ?event=B:Connect&time=1307118633&date=20110603-163033&ref=b52c3605e909d311bdbc0090331e0532&dir=out&src_if=BRI1&dst_if=GW1&src_cgpn=05123452006012&src_cdpn=6014&dst_cgpn=05123452006012&dst_cdpn=6014&dst_url=hre@datentechnik.com&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118630&connect_time=1307118633&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:30.000 PM*	*Jun 3 18:30:30 172.25.96.30 ?event=B:Alert&time=1307118630&date=20110603-163030&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118630&srv_i*

	d=00-90-33-1e-05-32
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=B:Alert&time=1307118630&date=20110603-163030&ref=b52c3605e909d311bdbc0090331e0532&dir=out&src_if=BRI1&dst_if=GW1&src_cgpn=05123452006012&src_cdpn=6014&dst_cgpn=05123452006012&dst_cdpn=6014&dst_url=hre@datentechnik.com&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&alert_time=1307118630&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=Media&time=1307118630&date=20110603-163030&ref=b52c3605e909d311bdbc0090331e0532&src_if=BRI1&dst_if=GW1&src_cgpn=05123452006012&src_cdpn=6014&dst_cgpn=05123452006012&dst_cdpn=6014&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=B:Call&time=1307118630&date=20110603-163030&ref=b52c3605e909d311bdbc0090331e0532&dir=out&src_if=BRI1&dst_if=GW1&src_cgpn=05123452006012&src_cdpn=6014&dst_cgpn=05123452006012&dst_cdpn=6014&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=A:Call&time=1307118630&date=20110603-163030&ref=b52c3605e909d311bdbc0090331e0532&dir=in&src_if=BRI1&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=Media&time=1307118630&date=20110603-163030&ref=0b7af455e909d311bdbc0090331e0532&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=G711A,30(0,0,0)&rcoder=G711A,30(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=B:Proceed&time=1307118630&date=20110603-163030&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=B:Call&time=1307118629&date=20110603-163029&ref=0b7af455e909d311bdbc0090331e0532&dir=out&src_if=GW1&dst_if=BRI1&src_cgpn=6012&src_cdpn=05123452006014&src_name=Schwanninger+F.&src_url=fsc@datentechnik.com&dst_cgpn=6012&dst_cdpn=05123452006014&src_reg_name=ATINN1+Trunk&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:30:29.000 PM*	*Jun 3 18:30:29 172.25.96.30 ?event=A:Call&time=1307118629&date=20110603-163029&ref=0b7af455e909d311bdbc0090331e0532&dir=in&src_if=GW1&bcaps=03_80_90_a3&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&srv_id=00-90-33-1e-05-32*
06.03.2011 *6:29:52.000 PM*	*Jun 3 18:29:52 172.25.29.30 ?event=A:Rel&time=1307118591&date=20110603-162951&ref=bb7fb7f1e909d311ae79009033105e11&dir=in&src_if=GW2&src_cgpn=4026&src_cdpn=4031&src_name=Drschka+Th.&src_url=tdr@datentechnik.com&dst_cgpn=4026&src_reg_name=ATVIE1-DT+Extern&bcaps=02_a8_80&xcoder=-,0(0,0,0)&rcoder=-,0(0,0,0)&xstats=0+0+0+0+0&rstats=0+0+0+0+0&disc_time=1307118591&srv_id=00*

	-90-33-08-02-d5

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Innsbruck, den 25.06.2011

Franz Schwanninger